J. Eur. Math. Soc. 15, 775–803

DOI 10.4171/JEMS/376

David L. Wehlau

Invariants for the modular cyclic group of prime order via classical invariant theory

Received October 7, 2010 and in revised form October 16, 2011

Abstract. Let $\mathbb{F}$ be any field of characteristic p. It is well-known that there are exactly p inequivalent indecomposable representations $V_1, \dots, V_p$ of C_p defined over $\mathbb{F}$. Thus if V is any finite-dimensional C_p-representation there are non-negative integers $0 \le n_1, \dots, n_k \le p-1$ such that $V \cong \bigoplus_{i=1}^k V_{n_i+1}$. It is also well-known that there is a unique (up to equivalence) $d+1$-dimensional irreducible complex representation of $\mathrm{SL}_2(\mathbb{C})$ given by its action on the space R_d of d-forms. Here we prove a conjecture, made by R. J. Shank, which reduces the computation of the ring of C_p-invariants $\mathbb{F}[\bigoplus_{i=1}^k V_{n_i+1}]^{C_p}$ to the computation of the classical ring of invariants (or covariants) $\mathbb{C}[R_1 \oplus \bigoplus_{i=1}^k R_{n_i}]^{\mathrm{SL}_2(\mathbb{C})}$. This shows that the problem of computing modular C_p-invariants is equivalent to the problem of computing classical $\mathrm{SL}_2(\mathbb{C})$-invariants. This allows us to compute for the first time the ring of invariants for many representations of C_p. In particular, we easily obtain from this generators for the rings of vector invariants $\mathbb{F}[mV_2]^{C_p}$, $\mathbb{F}[mV_3]^{C_p}$ and $\mathbb{F}[mV_4]^{C_p}$ for all $m \in \mathbb{N}$. This is the first computation of the latter two families of rings of invariants.

Keywords. Modular invariant theory, cyclic group, classical invariant theory, Roberts' isomorphism

1. Introduction

Let B be a domain and G a finite group. Consider a BG-module V which is a free B-module of rank n. We write $B[V]$ to denote the symmetric algebra $\mathrm{Sym}_B^\bullet(V^*)$ on the dual V^*. If we fix a basis $\{x_1, \dots, x_n\}$ for V^* we may identify $B[V]$ with the polynomial ring $B[x_1, \dots, x_n]$. The action of G on V induces an action of G on V^*. Extending this action algebraically we get a natural action of G on $B[V]$. We write $B[V]^G$ to denote the subring of invariants:

$$B[V]^G := \{f \in \mathbb{F}[V] \mid g \cdot f = f \ \forall g \in G\}.$$

Emmy Noether [33, 34] proved that the ring $B[V]^G$ is always finitely generated when B is a field (and G is finite).

We are concerned here with finding generators for the ring of invariants when $B = \mathbb{F}$ is a field of characteristic p and $G = C_p$ is the cyclic group of order p. We want to describe generating sets for $\mathbb{F}[V]^{C_p}$ not just for certain values of p but rather for arbitrary primes p.

D. L. Wehlau: Department of Mathematics and Computer Science, Royal Military College, Kingston, Ontario, Canada K7K 5L0; e-mail: wehlau@rmc.ca

The group C_p has, up to equivalence, exactly p indecomposable representations over $\mathbb{F}$. There is one indecomposable representation V_n of dimension n for every $n = 1, \ldots, p$. The representation V_1 is the trivial representation and V_p is the regular representation. If V contains a copy of V_1 as a summand, say $V = V_1 \oplus V'$, then it is easy to see that $\mathbb{F}[V]^{C_p} = \mathbb{F}[V_1] \otimes \mathbb{F}[V']^{C_p}$. For this reason it suffices to consider representations V which do not contain V_1 as a summand. Such a representation is called *reduced*. In order to simplify the exposition we will assume that our representations of C_p are reduced.

In 1913, L. Dickson [22] computed the rings of invariants $\mathbb{F}[V_2]^{C_p}$ and $\mathbb{F}[V_3]^{C_p}$. In 1990, David Richman [36] conjectured a set of generators for $\mathbb{F}[V_2 \oplus \cdots \oplus V_2]^{C_p}$ (for any number of copies of V_2). Campbell and Hughes [18] proved in 1997 that Richman's conjectured set of generators was correct.

In 1998, Shank [40] introduced a new method exploiting SAGBI bases and found generating sets for the two rings of invariants $\mathbb{F}[V_4]^{C_p}$ and $\mathbb{F}[V_5]^{C_p}$. In 2002, Shank and Wehlau [42] extended Shank's method to find generators for $\mathbb{F}[V_2 \oplus V_3]^{C_p}$. Since then, Shanks's method has been used to find generators for $\mathbb{F}[V_3 \oplus V_3]^{C_p}$ ([17]) and for $\mathbb{F}[V_2 \oplus V_2 \oplus V_3]^{C_p}$ ([23]). Limitations of the method using SAGBI bases imply that it seems infeasible to use the method to compute invariants for any further representation of C_p except probably $\mathbb{F}[V_2 \oplus V_4]^{C_p}$. See [41] and [17] for discussions of some of these limitations. Thus $\mathbb{F}[V]^{C_p}$ is known (for general p) only for the infinite family $V = mV_2 = \bigoplus^m V_2$ and for seven other small representations.

There is a deep connection between the invariants of C_p in characteristic p and the classical invariants of $\mathrm{SL}_2(\mathbb{C})$. This connection was pointed out and studied extensively by Gert Almkvist. See [2–7, 9].

Here we prove a conjecture of R. J. Shank which reduces the computation of generators for $\mathbb{F}[V]^{C_p}$ to the classical problem of computing $\mathbb{C}[W]^{\mathrm{SL}_2(\mathbb{C})}$. Here W is a representation of $\mathrm{SL}_2(\mathbb{C})$ which is easily obtained from V and with $\dim_{\mathbb{C}} W = \dim_{\mathbb{F}} V + 2$. The invariant ring $\mathbb{C}[W]^{\mathrm{SL}_2(\mathbb{C})}$ is called a ring of covariants (definition below). Since generators for $\mathbb{F}[V]^{C_p}$ yield generators for $\mathbb{C}[W]^{\mathrm{SL}_2(\mathbb{C})}$, our proof of this conjecture demonstrates the equivalence of these two problems.

After giving our proof of the conjecture we use the computation of $\mathbb{C}[W]^{\mathrm{SL}_2(\mathbb{C})}$ by classical invariant-theorists (and others) for a number of rings of covariants to give generators for the corresponding rings $\mathbb{F}[V]^{C_p}$. This greatly extends the above list of representations of C_p whose rings of invariants are known.

2. Preliminaries

We consider the $n \times n$ matrix with all eigenvalues equal to 1 and consisting of a single Jordan block:

$$\sigma_n(B) := \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 & 0 \\ 1 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & 0 & \ldots & 1 & 1 \end{pmatrix}_{n \times n}$$

where the entries of the matrix are elements of the ring B. Thus $\sigma_n(B) \in \mathrm{GL}_n(B)$.

The matrix $\sigma_n(B)$ generates a cyclic subgroup of $\mathrm{GL}_n(B)$. If the characteristic of B is 0 then $\sigma_n(B)$ has infinite order and so generates a group isomorphic to $\mathbb{Z}$. It is not too hard to see that if the characteristic of B is $p > 0$ then the order of $\sigma_n(B)$ is p^r where r is the least non-negative integer such that $p^r \geq n$.

2.1. *Certain $\mathbb{Z}$-modules*

We write M_n to denote the n-dimensional $\mathbb{Q}$-vector space which is a $\mathbb{Z}$-module where $1 \in \mathbb{Z}$ is represented by the matrix $\sigma_n(\mathbb{Q})$. It is easy to see that this $\mathbb{Z}$-module satisfies $M_n^* \cong M_n$.

We fix a basis of M_n with respect to which the matrix takes its given form. We write $M_n(\mathbb{Z})$ to denote the rank n lattice in M_n generated by integer linear combinations of this fixed basis. Thus $M_n(\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Q} = M_n$. The action of $\mathbb{Z}$ on M_n restricts to an action of $\mathbb{Z}$ on $M_n(\mathbb{Z})$. We write σ to denote $\sigma_n(\mathbb{Z})$ and Δ to denote $\sigma - 1$, an element of the group algebra.

Note that the one-dimensional $\mathbb{Q}$-vector space $M_n^{\mathbb{Z}}$ is the kernel of the map $\Delta : M_n \to M_n$. Given $W \cong \bigoplus_{i=1}^{s} M_{n_i}$ and $\omega \in W^{\mathbb{Z}}$ we say that the *length* of ω is r and write $\ell(\omega) = r$ to indicate that r is maximal such that $\omega \in \Delta^{r-1}(W)$.

2.2. *C_p-modules in characteristic p*

The book [20] includes a description of the representation theory of C_p over a field of characteristic p. We use σ to denote a generator of the group C_p. We also consider $\Delta := \sigma - 1$, an element of the group algebra of C_p. Whether σ is a generator of $\mathbb{Z}$ or C_p will be clear from the context. Similarly the meaning of Δ will be clear from the context.

Up to isomorphism, there is one indecomposable C_p-module of dimension n for each $1 \leq n \leq p$. We denote this module by V_n. Note that $V_n \cong V_n^*$. Also V_n is projective if and only if it is free if and only if $n = p$.

Since the group C_p is generated by a single element all of whose eigenvalues are 1, it follows that every C_p-module V is in fact defined over the prime field $\mathbb{F}_p \subseteq \mathbb{F}$. Thus if we let $V(\mathbb{F}_p)$ denote the $\mathbb{F}_p$-points of V we have $V = V(\mathbb{F}_p) \otimes_{\mathbb{F}_p} \mathbb{F}$. Since $\mathbb{F}[V]^{C_p}$ is the kernel of the linear operator $\Delta : \mathbb{F}[V] \to \mathbb{F}[V]$ we see that $\mathbb{F}[V]^{C_p} = (\mathbb{F}_p[V(\mathbb{F}_p)]^{C_p}) \otimes_{\mathbb{F}_p} \mathbb{F}$. Therefore it suffices to work over the prime field $\mathbb{F}_p$. We do this from now on.

Usually V_n is defined as the n-dimensional $\mathbb{F}_p$-module with the action of σ given by the matrix $\sigma_n(\mathbb{F}_p)$. We will use an equivalent description that is somewhat less common. We will realize V_n as the quotient ring $\mathbb{F}_p[t]/(t^n)$ equipped with a C_p-action by declaring that σ acts via multiplication by $1 + t$. Of course with respect to the basis of monomials in t, the matrix representation of multiplication by $1+t$ is $\sigma_n(\mathbb{F}_p)$. We use this description of V_n since it has an obvious grading given by polynomial degree. More precisely, given an element of $\mathbb{F}_p[t]/(t^n)$ we use its unique representation as a linear combination of $\{1, t, t^2, \ldots, t^{n-1}\}$ in order to give it a well-defined degree. We will use this polynomial degree to realize a filtration of V_n. We define $\mathcal{F}_r(V_n) := \{h \in \mathbb{F}_p[t]/(t^n) \mid \deg(h) \geq r\}$ for $0 \leq r \leq n$. Then $\{0\} = \mathcal{F}_n(V_n) \subset \mathcal{F}_{n-1}(V_n) \subset \cdots \subset \mathcal{F}_0(V_n) = V_n$.

Any element of $V_n \setminus \Delta(V_n)$ generates the cyclic C_p-module V_n. Let α denote such a generator and define $\omega := \Delta^{n-1}(\alpha)$. Then $V_n^{C_p}$, the socle of V_n, is spanned by ω. Given a C_p-module W and $\omega \in W^{C_p}$ we define $\ell(\omega)$ to be the maximum integer r such that $\omega \in \Delta^{r-1}(W)$. This integer $\ell(\omega)$ is called the *length* of ω.

2.3. Reduction modulo p

Let p be a prime integer. Since $M_n(\mathbb{Z})$ is a free $\mathbb{Z}$-module of rank n, reduction modulo p yields a surjective map $\rho : M_n(\mathbb{Z}) \to V := \mathbb{F}_p^n$. The action of $\mathbb{Z}$ on $M_n(\mathbb{Z})$ (generated by the action of $\sigma_n(\mathbb{Z})$) induces an action on V (generated by the action of $\sigma_n(\mathbb{F}_p)$). Suppose now that $1 < n \leq p$ so that $\sigma_n(\mathbb{F}_p)$ has order p and so gives an action of C_p on V. This action of C_p on V is indecomposable and therefore $V \cong V_n$ as a C_p-module. Thus reduction modulo p yields a surjective map $\rho : M_n(\mathbb{Z}) \to V_n$. Both M_n and V_n are self-dual and thus reduction modulo p is also surjective on the duals: $\rho : M_n^*(\mathbb{Z}) \to V_n^*$. This map of duals in turn induces a surjective map of coordinate rings

$$\rho : \mathrm{Sym}^\bullet_{\mathbb{Z}}(M_n^*(\mathbb{Z})) = \mathbb{Z}[M_n(\mathbb{Z})] \to \mathbb{F}_p[V_n] = \mathrm{Sym}^\bullet_{\mathbb{F}}(V^*).$$

More generally, reduction modulo p gives a surjection

$$\rho : \mathbb{Z}\Big[\bigoplus_{i=1}^k M_{n_i}(\mathbb{Z})\Big] \to \mathbb{F}_p\Big[\bigoplus_{i=1}^k V_{n_i}\Big].$$

Since $\rho \circ \sigma_n(\mathbb{Q}) = \sigma_n(\mathbb{F}_p) \circ \rho$ we see that

$$\rho\Big(\mathbb{Z}\Big[\bigoplus_{i=1}^k M_{n_i}(\mathbb{Z})\Big]^{\mathbb{Z}}\Big) \subseteq \mathbb{F}_p\Big[\bigoplus_{i=1}^k V_{n_i}\Big]^{C_p}.$$

Since C_p is not linearly reductive (over $\mathbb{F}_p$) this may in fact be a proper inclusion. We call the elements of $\rho(\mathbb{Z}[\bigoplus_{i=1}^k M_{n_i}(\mathbb{Z})]^{\mathbb{Z}})$ *integral invariants*. We caution the reader that Shank [40, 41] calls elements of $\mathbb{Z}[\bigoplus_{i=1}^k M_{n_i}(\mathbb{Z})]^{\mathbb{Z}}$ integral invariants and elements of $\rho(\mathbb{Z}[\bigoplus_{i=1}^k M_{n_i}(\mathbb{Z})]^{\mathbb{Z}})$ rational invariants.

2.4. Invariants of C_p

Let V be a C_p-representation. For each $f \in \mathbb{F}_p[V]$ we define an invariant called the *transfer* or *trace* of f, denoted $\mathrm{Tr}(f)$, by

$$\mathrm{Tr}(f) := \sum_{\tau \in C_p} \tau f.$$

Similarly we define the *norm* of f, denoted $N^{C_p}(f)$, by

$$N^{C_p}(f) := \prod_{\tau \in C_p} \tau f.$$

Consider a representation $V = V_{n_1} \oplus \cdots \oplus V_{n_r}$ of C_p. For each summand V_{n_i} choose a generator z_i of the dual cyclic C_p-module $V_{n_i}^*$, i.e., choose $z_i \in V_{n_i}^* \setminus \Delta(V_{n_i}^*)$. Define $N_i := N^{C_p}(z_i)$ for $i = 1, \ldots, r$. Later we will study C_p-invariants using a term order.

For a summary of term orders see [21, Chapter 2]. We will always use a graded reverse lexicographic order with $z_i > \Delta(z_i) > \cdots > \Delta^{n_i-1}(z_i)$ for all $i = 1, \ldots, r$. We denote the lead term of an element $f \in \mathbb{F}_p[V]$ by $\mathrm{LT}(f)$ and the lead monomial of f by $\mathrm{LM}(f)$. We follow the convention that a monomial is a product of variables.

3. The conjecture

Let $V = V_{n_1} \oplus \cdots \oplus V_{n_r}$ be a C_p-module. We have seen three ways to construct C_p-invariants: norms, traces and integral invariants. R. J. Shank [40, Conjecture 6.1] conjectured that $\mathbb{F}_p[V]^{C_p}$ is generated by the norms $N_1, \ldots, N_r$ together with a finite set of integral invariants and a finite set of transfers. Originally Shank stated his conjecture only for V indecomposable but he later asserted it for general C_p-modules ([41, §3]). Our main result here is to prove this conjecture. We then apply the result to obtain generating sets for a number of C_p-modules V.

4. Classical invariant theory of $\mathrm{SL}_2(\mathbb{C})$

Here we consider representations of the classical group $\mathrm{SL}_2(\mathbb{C})$. There are many good introductions to this topic. For our purposes the book by Procesi [35] is especially well suited since it emphasizes an invariant-theoretic approach. The results of this section are well-known.

Let R_1 denote the defining representation of $\mathrm{SL}_2(\mathbb{C})$ with basis $\{X, Y\}$. Define $R_d := \mathrm{Sym}^d(R_1)$ to be the space of homogeneous forms of degree d in X and Y. The action of $\mathrm{SL}_2(\mathbb{C})$ on R_1 induces an action on R_d. This action[1] is given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot f(X, Y) = f(aX + cY, bX + dY).$$

Gordan [28] showed that the algebra $\mathbb{C}[W]^{\mathrm{SL}_2(\mathbb{C})}$ is finitely generated for any finite-dimensional representation W of $\mathrm{SL}_2(\mathbb{C})$. The algebra $(\mathrm{Sym}^\bullet(R_1) \otimes \mathbb{C}[W])^{\mathrm{SL}_2(\mathbb{C})}$ is known as the *ring of covariants* of W. This ring was a central object of study in classical invariant theory. Since the representations R_1 and R_1^* are equivalent, it follows that $(\mathrm{Sym}^\bullet(R_1) \otimes \mathbb{C}[W])^{\mathrm{SL}_2(\mathbb{C})} \cong \mathbb{C}[R_1 \oplus W]^{\mathrm{SL}_2(\mathbb{C})}$. We will also refer to this latter ring as the ring of covariants of W. Classical invariant-theorists found generators for the rings of covariants of a number of small representations W of $\mathrm{SL}_2(\mathbb{C})$.

We work with the basis $\{x, y\}$ of R_1^* which is dual to the basis $\{Y, X\}$ of R_1. Then $\sigma(x) = y - x$ and $\sigma(y) = y$. We also use $\left\{\binom{d}{i} a_i \mid i = 0, 1, \ldots, n\right\}$ as a basis for R_d^* where $\{a_0, a_1, \ldots, a_d\}$ is dual to $\{X^d, -X^{d-1}Y, \ldots, X^{d-i}(-Y)^i, \ldots, Y^d\}$. We choose these bases in order that the homogeneous d-form

$$f = \sum_{i=0}^{n} \binom{d}{i} a_i x^{d-i} y^i \in (R_1 \oplus R_d)^*$$

[1] In fact, classically the formula used was $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot f(X, Y) = f(aX + bY, cX + dY)$. This yields a right action and since we prefer left actions we use the other formula. It is clear the two actions are equivalent and have the same ring of invariants.

is invariant under the action of $\mathrm{SL}_2(\mathbb{C})$. Putting $f = \sum_{i=0}^{n} \binom{d}{i} a_1 x^{d-i} y^i$ into the above formula for the action we find that $\sigma = \sigma_2(\mathbb{C})$ acts on R_d^* via $\sigma(a_r) = \sum_{j=0}^{r} \binom{r}{j} a_j$ for $r = 0, 1, \ldots, d$. From this it is easy to see that σ acts irreducibly on R_d^*. It can be shown that R_d and R_d^* are equivalent as representations of $\mathrm{SL}_2(\mathbb{C})$. In fact, if W is any irreducible representation of $\mathrm{SL}_2(\mathbb{C})$ of dimension $d+1$ then W is equivalent to R_d. Since σ acts irreducibly on R_d, it follows that the action of σ on R_d is given (with respect to a Jordan basis) by $\sigma_{d+1}(\mathbb{C})$.

Given two forms $g \in R_m = \mathrm{Sym}^m(R_1)$ and $h \in R_n = \mathrm{Sym}^n(R_1)$, their r^{th} *transvectant* is defined by

$$(g,h)^r := \frac{(m-r)!(n-r)!}{m!n!} \sum_{i=0}^{r} (-1)^i \binom{r}{i} \frac{\partial^r g}{\partial X^{r-i} \partial Y^i} \frac{\partial^r h}{\partial X^i \partial Y^{r-i}}$$

for $r = 0, 1, \ldots, \min\{m,n\}$. It has degree (traditionally called *order*) $m+n-2r$ in X, Y, i.e., $(g,h)^r \in R_{m+n-2r}$.

The Clebsch–Gordan formula [35, §3.3] asserts that

$$R_m \otimes R_n \cong \bigoplus_{r=0}^{\min\{m,n\}} R_{m+n-2r}.$$

If $g \in R_m$ and $h \in R_n$ then the projection of $R_m \otimes R_n$ onto its summand R_{m+n-2r} carries $g \otimes h$ onto $(g,h)^r$.

Example 4.1. The ring of covariants of $W = R_2 \oplus R_3$ was computed by classical invariant-theorists. In this example, we concentrate on $\mathbb{C}[R_1 \oplus R_2 \oplus R_3]^{\mathrm{SL}_2(\mathbb{C})}_{(*,1,1)}$. In [29, §140] it is shown that the ring $\mathbb{C}[R_1 \oplus R_2 \oplus R_3]^{\mathrm{SL}_2(\mathbb{C})}$ is generated by 15 generators. Following the notation there, we use ϕ to denote an element of R_2 (the quadratic) and f to denote an element of R_3 (the cubic). Examining the multi-degrees of the 15 generators we find that four of them are relevant to understanding $\mathbb{C}[R_1 \oplus R_2 \oplus R_3]^{\mathrm{SL}_2(\mathbb{C})}_{(*,1,1)}$. These are $(\phi, f)^1$ of degree $(3,1,1)$, $(\phi, f)^2$ of degree $(1,1,1)$ and the two forms ϕ of degree $(2,1,0)$ and f of degree $(3,0,1)$. Thus $\mathbb{C}[R_1 \oplus R_2 \oplus R_3]^{\mathrm{SL}_2(\mathbb{C})}_{(*,1,1)}$ is 3-dimensional with basis $\{(\phi, f)^1, (\phi, f)^2, \phi f\}$.

5. Roberts' isomorphism

Given a covariant $g = g_0 Y^d + g_1 X Y^{d-1} + \cdots + g_d X^d$, the coefficient g_0 of Y^d is called the *source* of g and is also known as a *semi-invariant*.

Let W be any representation of $\mathrm{SL}_2(\mathbb{C})$. *Roberts' isomorphism* (see [37]) is the isomorphism which associates to a covariant its source:

$$\psi : \mathbb{C}[R_1 \oplus W]^{\mathrm{SL}_2(\mathbb{C})} \to \mathbb{C}[W]^H$$

given by $\psi(f(\cdot,\cdot)) = f(Y,\cdot)$ where R_1 has basis $\{X, Y\}$ and H is the subgroup

$$H := \mathrm{SL}_2(\mathbb{C})_Y = \{\alpha \in \mathrm{SL}_2(\mathbb{C}) \mid \alpha \cdot Y = Y\} = \left\{ \begin{pmatrix} 1 & 0 \\ z & 1 \end{pmatrix} \;\middle|\; z \in \mathbb{C} \right\}$$

which fixes Y. For a modern discussion and proof of Roberts' isomorphism see [16] or [35, §15.1.3, Theorem 1].

Clearly H contains a copy K of the integers $\mathbb{Z}$ as a dense (in the Zariski topology) subgroup: $K := \left\{ \left(\begin{smallmatrix} 1 & 0 \\ m & 1 \end{smallmatrix}\right) \mid m \in \mathbb{Z} \right\}$. This is just the subgroup of $\mathrm{GL}_2(\mathbb{C})$ generated by $\sigma_2(\mathbb{C})$. Since K is dense in H, we have $\mathbb{C}[W]^H = \mathbb{C}[W]^K$ and thus $\mathbb{C}[R_1 \oplus W]^{\mathrm{SL}_2(\mathbb{C})} \cong \mathbb{C}[W]^K$.

Since the action of K on W is defined over $\mathbb{Z} \subset \mathbb{Q}$ we have

$$W \cong W(\mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{C} \cong W(\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{C}$$

where $W(\mathbb{Z})$ denotes the integer points of W and $W(\mathbb{Q}) \cong W(\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Q}$ denotes the $\mathbb{Q}$-points of W.

Thus

$$\mathbb{C}[R_1 \oplus W]^{\mathrm{SL}_2(\mathbb{C})} \cong \mathbb{C}[W]^H = \mathbb{C}[W]^K$$

As above, $\mathbb{C}[W]^K$ is the kernel of the linear operator $\Delta : \mathbb{C}[W] \to \mathbb{C}[W]$ and thus

$$\mathbb{C}[W]^K \cong \mathbb{Q}[W(\mathbb{Q})]^K \otimes_{\mathbb{Q}} \mathbb{C} \cong (\mathbb{Z}[W(\mathbb{Z})]^K \otimes_{\mathbb{Z}} \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{C} \cong \mathbb{Z}[W(\mathbb{Z})]^K \otimes_{\mathbb{Z}} \mathbb{C}.$$

Clearly $R_d(\mathbb{Q})$ is isomorphic to the $\mathbb{Z}$-module M_{d+1} considered above. Thus we may identify M_{d+1} with the $\mathbb{Q}$-points of R_d and $M_{d+1}(\mathbb{Z})$ with the $\mathbb{Z}$-points of R_d. Writing $W \cong \bigoplus_{i=1}^k R_{d_i}$ we have

$$\mathbb{C}\Big[R_1 \oplus \bigoplus_{i=1}^k R_{d_i}\Big]^{\mathrm{SL}_2(\mathbb{C})} \cong \mathbb{Q}\Big[\bigoplus_{i=1}^k M_{d_i+1}\Big]^{\mathbb{Z}} \otimes_{\mathbb{Q}} \mathbb{C} \cong \mathbb{Z}\Big[\bigoplus_{i=1}^k M_{d_i+1}(\mathbb{Z})\Big]^{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{C}.$$

(Here we are writing $\mathbb{Z}$ for the group K.) Furthermore

$$\rho : \mathbb{Z}\Big[\bigoplus_{i=1}^k M_{d_i+1}(\mathbb{Z})\Big]^{\mathbb{Z}} \to \mathbb{F}_p\Big[\bigoplus_{i=1}^k V_{d_i+1}\Big]^{C_p}$$

where the kernel of ρ is the principal ideal generated by p.

6. Periodicity

Let V be a C_p-module and write V as a direct sum of indecomposable C_p-modules: $V = V_{n_1} \oplus \cdots \oplus V_{n_r}$. This decomposition induces an $\mathbb{N}^r$-grading on $\mathbb{F}_p[V]$ which is preserved by the action of C_p. As above we choose a generator $z_i \in V_{n_i}^*$ for each $i = 1, \ldots, r$ and put $N_i := N^{C_p}(z_i)$. We further define $\mathbb{F}_p[V]^\sharp$ to be the ideal of $\mathbb{F}_p[V]$ generated by $N_1, \ldots, N_r$.

The following theorem (see for example [42, §2]) is very useful.

Theorem 6.1 (Periodicity). *The ideal $\mathbb{F}_p[V]^\sharp$ is a summand of the C_p-module $\mathbb{F}_p[V]$. Denoting its complement by $\mathbb{F}_p[V]^\flat$ we have the decomposition $\mathbb{F}_p[V] = \mathbb{F}_p[V]^\sharp \oplus \mathbb{F}_p[V]^\flat$ as C_p-modules. Taking the multi-grading into account we have*

$$\mathbb{F}_p[V]_{(d_1,\ldots,d_r)} = \mathbb{F}_p[V]^\sharp_{(d_1,\ldots,d_r)} \oplus \mathbb{F}_p[V]^\flat_{(d_1,\ldots,d_r)}.$$

Moreover if there exists i such that $d_i \geq p - n_i + 1$ then $\mathbb{F}_p[V]^\flat_{(d_1,\ldots,d_r)}$ is a free C_p-module.

Remark 6.2. More can be said: in fact,

$$\mathbb{F}_p[V]_{(d_1,\dots,d_i-1,d_i+p,d_{i+1},\dots,d_r)} \cong \mathbb{F}_p[V]_{(d_1,\dots,d_r)} \oplus kV_p$$

for some positive integer k. This explains why the previous theorem is known by the name *periodicity*.

The decomposition given by the periodicity theorem obviously yields a vector space decomposition of the multi-graded ring of invariants:

$$\mathbb{F}_p[V]^{C_p}_{(d_1,\dots,d_r)} = (\mathbb{F}_p[V]^{C_p}_{(d_1,\dots,d_r)})^\sharp \oplus (\mathbb{F}_p[V]^{C_p}_{(d_1,\dots,d_r)})^\flat.$$

Here

$$(\mathbb{F}_p[V]^{C_p}_{(d_1,\dots,d_r)})^\sharp = (\mathbb{F}_p[V]^\sharp_{(d_1,\dots,d_r)}) \cap \mathbb{F}_p[V]^{C_p}$$

is the ideal of $\mathbb{F}_p[V]^{C_p}$ generated by $N_1, \dots, N_r$ and

$$(\mathbb{F}_p[V]^{C_p}_{(d_1,\dots,d_r)})^\flat = (\mathbb{F}_p[V]^\flat_{(d_1,\dots,d_r)}) \cap \mathbb{F}_p[V]^{C_p}.$$

7. Outline of the proof

We are now in a position to outline the main steps of our proof. We want to show that the cokernel of the reduction mod p map $\rho : \mathbb{Z}[\bigoplus_{i=1}^r M_{n_i}(\mathbb{Z})]^{\mathbb{Z}} \to \mathbb{F}_p[\bigoplus_{i=1}^r V_{n_i}]^{C_p}$ is spanned by products of transfers and the norms $N_1, \dots, N_r$. We consider a fixed multi-degree $(d_1, \dots, d_n)$. Using the Periodicity Theorem we may reduce to the case where $d_i < p$ for each i. Then we may exploit the fact that for such values of d_i the homogeneous component $\mathbb{F}_p[\bigoplus_{i=1}^r V_{n_i}]_{(d_1,\dots,d_n)}$ is a summand of $\bigotimes_{i=1}^r \bigotimes^{d_i} V_{n_i}$. Thus we may consider the reduction mod p map $\rho : \bigotimes_{i=1}^r \bigotimes^{d_i} M_{n_i}(\mathbb{Z}) \to \bigotimes_{i=1}^r \bigotimes^{d_i} V_{n_i}$. For this map we will show that for any summand V_k of $\bigotimes_{i=1}^r \bigotimes^{d_i} V_{n_i}$ with $k < p$, there exists a corresponding summand M_k of $\bigotimes_{i=1}^r \bigotimes^{d_i} M_{n_i}$ with $\rho(M_k(\mathbb{Z})) = V_k$. In particular $V_k^{C_p}$ lies in the image of ρ. By induction we reduce to $\rho : M_m(\mathbb{Z}) \otimes M_n(\mathbb{Z}) \to V_m \otimes V_n$ where $m, n \le p$. By carefully examining explicit decompositions of $M_m \otimes M_n$ and $V_m \otimes V_n$ we are able to show that any summand V_k of $V_m \otimes V_n$ is contained $\rho(M_m(\mathbb{Z}) \otimes M_n(\mathbb{Z}))$.

The following example is instructive as regards both dependence on the prime p and our solution to the last step in the above outline of the proof.

Example 7.1. We consider the $\mathbb{Z}$-module $M_3 \otimes M_4$. We realize M_3 as $\mathbb{Q}[s]/(s^3)$ and M_4 as $\mathbb{Q}[t]/(t^4)$ with $\Delta(s^i) = s^{i+1}$ and $\Delta(t^j) = t^{j+1}$. By (8.1) we have $M_3 \otimes M_4 \cong M_2 \oplus M_4 \oplus M_6$. We can also see this decomposition explicitly as follows. Let $\alpha_0 := 1$, $\alpha_1 := 3s - 2t$ and $\alpha_2 := 3s^2 - 2st + t^2 + 2t^3$. Then

$$\begin{aligned} \alpha_0 &:= 1, \\ \Delta(\alpha_0) &= s + t + st, \\ \Delta^2(\alpha_0) &= s^2 + 2st + t^2 + 2s^2t + 2st^2 + s^2t^2, \end{aligned}$$

$$\begin{aligned}
\Delta^3(\alpha_0) &= 3s^2t + 3st^2 + t^3 + 6s^2t^2 + 3st^3 + 3s^2t^3,\\
\Delta^4(\alpha_0) &= 6s^2t^2 + 4st^3 + 12s^2t^3,\\
\Delta^5(\alpha_0) &= 10s^2t^3,\\
\Delta^6(\alpha_0) &= 0,\\
\alpha_1 &:= 3s - 2t,\\
\Delta(\alpha_1) &= 3s^2 + st - 2t^2 + 3s^2t - 2st^2,\\
\Delta^2(\alpha_1) &= 4s^2t - st^2 + 2t^3 + 2s^2t^2 - 4st^3 + 2s^2t^3,\\
\Delta^3(\alpha_1) &= 3s^2t^2 - 3st^3 - 3s^2t^3,\\
\Delta^4(\alpha_1) &= 0,\\
\alpha_2 &:= 3s^2 - 2st + t^2 + 2t^3,\\
\Delta(\alpha_2) &= s^2t - st^2 + t^3 - 2s^2t^2 + 3st^3,\\
\Delta^2(\alpha_2) &= 0.
\end{aligned}$$

Thus $\operatorname{span}_{\mathbb{Q}}\{\alpha_2, \Delta(\alpha_2)\} \cong M_2$, $\operatorname{span}_{\mathbb{Q}}\{\Delta^j(\alpha_1) \mid 0 \le i \le 3\} \cong M_4$ and $\operatorname{span}_{\mathbb{Q}}\{\Delta^j(\alpha_0) \mid 0 \le i \le 5\} \cong M_6$. Hence we have an explicit decomposition: $M_3 \otimes M_4 \cong M_2 \oplus M_4 \oplus M_6$.

We put $\omega_0 := s^2t^3$, $\omega_1 := s^2t^2 - st^3 - s^2t^3$ and $\omega_2 := s^2t - st^2 + t^3 - 2s^2t^2 + 3st^3$. Thus $\omega_0 := \Delta^5(\alpha_0/10)$, $\omega_1 := \Delta^3(\alpha_1/3)$ and $\omega_2 := \Delta^1(\alpha_2)$. Therefore $\ell(\omega_0) = 6$, $\ell(\omega_1) = 4$ and $\ell(\omega_2) = 2$.

Take $p \ge 5$. Reduction modulo p gives the map $\rho : M_3(\mathbb{Z}) \otimes M_4(\mathbb{Z}) \to V_3 \otimes V_4$. From Proposition 8.4 we have

$$V_3 \otimes V_4 \cong \begin{cases} V_2 \oplus V_4 \oplus V_6 & \text{if } p \ge 7,\\ V_2 \oplus 2V_5 & \text{if } p = 5. \end{cases}$$

Again we may see this decomposition explicitly by considering the action of C_p on $V_3 \otimes V_4$ as follows.

Put $\overline{\omega}_i := \rho(\omega_i)$ and $\overline{\alpha}_i := \rho(\alpha_i)$ for $i = 0, 1, 2$.

First suppose that $p \ge 7$. Take $\mu_0, \mu_1 \in \mathbb{Z}$ with $10\mu_0 \equiv 1 \pmod p$ and $3\mu_1 \equiv 1 \pmod p$. Then from the above computations we have $\operatorname{span}_{\mathbb{F}_p}\{\overline{\alpha}_2, \Delta(\overline{\alpha}_2)\} \cong V_2$, $\operatorname{span}_{\mathbb{F}_p}\{\Delta^j(\mu_1\overline{\alpha}_1) \mid 0 \le i \le 3\} \cong V_4$ and $\operatorname{span}_{\mathbb{F}_p}\{\Delta^j(\mu_0\overline{\alpha}_0) \mid 0 \le i \le 5\} \cong V_6$. In particular, $\Delta^5(\mu_0\overline{\alpha}_0) = \overline{\omega}_0$, $\Delta^3(\mu_1\overline{\alpha}_1) = \overline{\omega}_i$ and $\Delta(\overline{\alpha}_2) = \overline{\omega}_2$ and therefore $\ell(\overline{\omega}_2) = 2 = \ell(\omega_2)$, $\ell(\overline{\omega}_1) = 4 = \ell(\omega_1)$ and $\ell(\overline{\omega}_0) = 6 = \ell(\omega_0)$.

Now we consider the case $p = 5$. Then $\Delta^5(\overline{\alpha}_0) = 0$ and from this we can show that $\overline{\omega}_0 \notin \Delta^5(V_3 \otimes V_4)$. Hence $\ell(\overline{\omega}_0) \le 5$. Here we may define $\overline{\beta}_0 := \rho(s)$, $\overline{\beta}_1 := 3\overline{\alpha}_0$ and $\overline{\beta}_2 := \rho(\alpha)_2$. Then $\operatorname{span}_{\mathbb{F}_5}\{\overline{\beta}_2, \Delta(\overline{\beta}_2)\} \cong V_2$, $\operatorname{span}_{\mathbb{F}_5}\{\Delta^j(\mu_1\overline{\beta}_1) \mid 0 \le i \le 4\} \cong V_5$ and $\operatorname{span}_{\mathbb{F}_5}\{\Delta^j(\mu_0\overline{\beta}_0) \mid 0 \le i \le 4\} \cong V_5$. Then $\Delta^4(\overline{\beta}_0) = \overline{\omega}_0$, $\Delta^4(\overline{\beta}_1) = \overline{\omega}_1$ and $\Delta(\overline{\beta}_2) = \overline{\omega}_2$. Thus $\ell(\overline{\omega}_0) = \ell(\overline{\omega}_1) = 5$ and $\ell(\overline{\omega}_2) = 2$.

Comparing this with Example 4.1 we see that (up to choice of bases) $\psi((\phi, f)^1) = \omega_1$, $\psi((\phi, f)^2) = \omega_2$ and $\psi(\phi f) = \omega_0$.

8. Representation rings

8.1. Complex representations of $\mathrm{SL}_2(\mathbb{C})$

Let $\mathrm{Rep}_{\mathbb{C}\,\mathrm{SL}_2(\mathbb{C})}$ denote the representation ring of complex representations of $\mathrm{SL}_2(\mathbb{C})$. Then

$$\mathrm{Rep}_{\mathbb{C}\,\mathrm{SL}_2(\mathbb{C})} \cong \mathbb{Z}[\widetilde{R}_1] \cong \bigoplus_{d=0}^{\infty} \mathbb{Z}\widetilde{R}_d.$$

Here $\widetilde{R}_d$ is a formal variable corresponding to the representation R_d for all $d \geq 1$ and $\widetilde{R}_0 = 1 \in \mathrm{Rep}_{\mathbb{C}\,\mathrm{SL}_2(\mathbb{C})}$ corresponds to the one-dimensional trivial representation. Multiplication in $\mathrm{Rep}_{\mathbb{C}\,\mathrm{SL}_2(\mathbb{C})}$ is given by the Clebsch–Gordan rule (see [35, §3.3])

$$\widetilde{R}_m \cdot \widetilde{R}_n = \sum_{k=0}^{\min\{m,n\}} \widetilde{R}_{|n-m|+2k}.$$

This formula can be used to inductively derive a formula expressing $\widetilde{R}_d$ as a polynomial in $\mathbb{Z}[\widetilde{R}_1]$. Almkvist [6, Theorem 1.4(a)] showed that in fact $\widetilde{R}_d = \mathrm{U}_{d+1}(\widetilde{R}_1/2)$ where $\mathrm{U}_n(x)$ is the n^{th} Chebyshev polynomial of the second kind.

8.2. Certain rational representations of $\mathbb{Z}$

Let $\mathrm{Rep}'_{\mathbb{Q}\,\mathbb{Z}}$ denote the subring of the representation ring of $\mathbb{Z}$ given by

$$\mathrm{Rep}'_{\mathbb{Q}\,\mathbb{Z}} := \mathbb{Z}[\widetilde{M}_2] \cong \bigoplus_{d=1}^{\infty} \mathbb{Z}\widetilde{M}_d.$$

Here $\widetilde{M}_d$ is a formal variable corresponding to the representation M_d for all $d \geq 2$ and $\widetilde{M}_1 = 1 \in \mathrm{Rep}'_{\mathbb{Q}\,\mathbb{Z}}$ corresponds to the one-dimensional trivial representation. The multiplication in $\mathrm{Rep}'_{\mathbb{Q}\,\mathbb{Z}}$ is given by a Clebsch–Gordan type formula:

$$\widetilde{M}_m \cdot \widetilde{M}_n = \bigoplus_{k=1}^{\min\{m,n\}} \widetilde{M}_{|n-m|+2k-1}. \tag{8.1}$$

This result is an immediate consequence of the Clebsch–Gordan formula for $R_{m-1} \otimes R_{n-1}$, after restricting from $\mathrm{SL}_2(\mathbb{C})$ to the subgroup $K \cong \mathbb{Z}$ and using Roberts' isomorphism as above. Alternatively, this result follows from the Jordan form of the Kronecker (or tensor) product of two matrices in Jordan form. Such a decomposition was given independently by Aiken [1] and Roth [38] in 1934. The proof by Aiken contains an error (the same error occurs in the treatment of this problem by Littlewood [31]). The proof by Roth has been criticized for not providing sufficient details for the so-called "hard case" when both matrices are invertible. This is precisely the case which may be settled by exploiting Roberts' isomorphism. Marcus and Robinson [32] gave a complete proof extending the ideas of Roth. In the words of Brualdi [15], "the difficult case (...) constitutes the most substantial part of [Marcus and Robinson's] proof". Brualdi [15]

gave a proof based on Aiken's method. Brualdi's article also includes a good discussion of the history of this problem. The approach via Roberts' isomorphism appears to have been overlooked by people studying this problem.

Again this formula can be used to inductively derive a formula expressing $\widetilde{M}_d$ as a polynomial in $\mathbb{Z}[\widetilde{M}_2]$. Once again the answer is given by a Chebyshev polynomial of the second kind: $\widetilde{M}_d = \mathrm{U}_d(\widetilde{M}_2/2)$.

8.3. Characteristic p representations of C_p

Let $\mathrm{Rep}_{\mathbb{F}_p C_p}$ denote the representation ring of C_p over the field $\mathbb{F}_p$.

The multiplication here is determined by

$$\widetilde{V}_2 \otimes \widetilde{V}_n \cong \begin{cases} \widetilde{V}_2 & \text{if } n = 1, \\ \widetilde{V}_{n-1} \oplus \widetilde{V}_{n+1} & \text{if } 2 \le n \le p-1, \\ 2\widetilde{V}_p & \text{if } n = p. \end{cases}$$

Here $\widetilde{V}_d$ is a formal variable corresponding to the representation V_d for all $2 \le d \le p$, and $\widetilde{V}_1 = 1 \in \mathrm{Rep}_{\mathbb{F}_p C_p}$ corresponds to the one-dimensional trivial representation. For an especially simple proof of this formula see the proof of [30, Lemma 2.2].

From this it follows that $\widetilde{V}_d = \mathrm{U}_d(\widetilde{V}_2/2)$ for $d \le p$, a fact also shown by Almkvist [3, Theorem 5.10(b)]. It is convenient to define $\widetilde{V}_d := \mathrm{U}_d(\widetilde{V}_2/2) \in \mathrm{Rep}_{\mathbb{F}_p C_p}$ for $d > p$.

The above formula implies that

$$\mathrm{Rep}_{\mathbb{F}_p C_p} \cong \mathbb{Z}[\widetilde{V}_2] \cong \mathbb{Z}[T]/q(T) \cong \bigoplus_{d=1}^{p} \mathbb{Z}\widetilde{V}_d$$

where q is a certain polynomial of degree p. For details see Almkvist's paper [6]. The polynomial q is determined by the fact that $\widetilde{V}_{p+1} - 2\widetilde{V}_p + \widetilde{V}_{p-1} = 0$. Thus $q(T) = \mathrm{U}_{p+1}(T/2) - 2\mathrm{U}_p(T/2) + \mathrm{U}_{p-1}(T/2)$.

Reduction modulo p carries the lattice $M_d(\mathbb{Z})$ to the representation V_d of C_{p^r} where $p^{r-1} < d \le p^r$. In particular, reduction modulo p carries $M_d(\mathbb{Z})$ to the representation V_d of C_p for all $d \le p$. Thus the map ρ, defined above, induces a map $\phi : \mathrm{Rep}'_{\mathbb{Q}\mathbb{Z}} \to \mathrm{Rep}_{\mathbb{F}_p C_p}$ given by $\phi(\widetilde{M}_2) = \widetilde{V}_2$. Also $\phi(\widetilde{M}_d) = \widetilde{V}_d$ for all $d = 1, \ldots, p$. In fact $\phi(\widetilde{M}_d) = \widetilde{V}_d$ for all $d \ge 1$ since $\widetilde{M}_d = \mathrm{U}_d(\widetilde{M}_2/2)$ for all $d \ge 1$.

With this convention the multiplication rule may be expressed in a form similar to the Clebsch–Gordan formula:

$$\widetilde{V}_m \cdot \widetilde{V}_n = \sum_{k=1}^{\min\{m,n\}} \widetilde{V}_{|n-m|+2k-1}. \tag{8.2}$$

It is clear that the map ϕ is a surjection whose kernel is the principal ideal generated by $q(\widetilde{M}_2)$.

We wish to derive a more enlightening and explicit formula for the product $\widetilde{V}_m \cdot \widetilde{V}_n$ for the cases corresponding to actual (indecomposable) representations, i.e., when $1 \le m, n \le p$. More precisely, we want to express such a product in terms of the elements $\widetilde{V}_d$ with $d \le p$.

We prove the following.

Proposition 8.4. *Let* $1 \leq m \leq n \leq p$. *Then*

$$\widetilde{V}_m \cdot \widetilde{V}_n = \begin{cases} \sum_{i=1}^{m} \widetilde{V}_{m+n-2i+1} = \sum_{s=1}^{m} \widetilde{V}_{n-m+2s-1} & \text{if } m+n \leq p+1, \\ \sum_{i=m+n-p+1}^{m} \widetilde{V}_{m+n-2i+1} + (m+n-p)\widetilde{V}_p & \\ \quad = \sum_{s=1}^{p-n} \widetilde{V}_{n-m+2s-1} + (m+n-p)\widetilde{V}_p & \text{if } m+n \geq p. \end{cases}$$

Proof. If $m+n \leq p+1$ then the result follows from the Clebsch–Gordan type formula (8.2) above.

Now we suppose that $m+n \geq p+2$. For this case, the proof is by induction on m. If $m=2$ then we must have $n=p$ since $m+n \geq p+2$. Hence $V_n = V_p$ is projective and therefore so is $V_m \otimes V_n$. This implies $V_m \otimes V_p \cong mV_p$. Thus the result is true for $m=2$.

Suppose then that the result holds for $m = 2, \ldots, r-1$ and we will prove it for $m = r$. Again, using projectivity, the result is clear if $m = p$ so we may suppose that $m = r \leq p-1$. Consider $\widetilde{V}_2 \cdot \widetilde{V}_{r-1} \cdot \widetilde{V}_n$. We have

$$\begin{aligned} (\widetilde{V}_2 \cdot \widetilde{V}_{r-1}) \cdot \widetilde{V}_n &= (\widetilde{V}_r + \widetilde{V}_{r-2}) \cdot \widetilde{V}_n = (\widetilde{V}_r \cdot \widetilde{V}_n) + (\widetilde{V}_{r-2} \cdot \widetilde{V}_n) \\ &= (\widetilde{V}_r \cdot \widetilde{V}_n) + \Big(\sum_{s=1}^{p-n} \widetilde{V}_{n-r+2s+1}\Big) + (r+n-p-2)\widetilde{V}_p \end{aligned}$$

since $r+n-2 \geq p$. On the other hand,

$$\begin{aligned} \widetilde{V}_2 \cdot (\widetilde{V}_{r-1} \cdot \widetilde{V}_n) &= \widetilde{V}_2 \cdot \Big(\sum_{s=1}^{p-n} \widetilde{V}_{n-r+2s} + (r+n-p-1)\,\widetilde{V}_p\Big) \\ &\qquad \text{since } r-1 \geq p-n+1 > p-n \\ &= \sum_{s=1}^{p-n} \widetilde{V}_{n-r+2s+1} + \sum_{s=1}^{p-n} \widetilde{V}_{n-r+2s-1} + 2(r+n-p-1)\,\widetilde{V}_p. \end{aligned}$$

Therefore $\widetilde{V}_r \cdot \widetilde{V}_n = \sum_{s=1}^{p-n} \widetilde{V}_{n-r+2s-1} + (r+n-p)\,\widetilde{V}_p$. □

Remark 8.5. Note that if $m \leq n \leq p$ then $\dim (V_m \otimes V_n)^{C_p} = m$ for both of the cases $m+n \leq p$ and $m+n > p$.

9. Explicit decompositions

The formulae in the previous section describe the decomposition of tensor products of representations abstractly. We will require more explicit decompositions including not just a list of the representations occurring in a product but also some information about how these subrepresentations lie in the tensor product. We will use the formulae from the representation rings to help in determining this extra information.

9.1. Decomposing $M_m \otimes M_n$

We begin by considering the product $M_m \otimes M_n$. Suppose $m \leq n$. From the representation ring formula we know that

$$M_m \otimes M_n \cong \bigoplus_{s=1}^{m} M_{n-m+2s-1}. \tag{9.1}$$

For our purposes we need an explicit description of the submodules occurring in this decomposition. We write

$$M_m \otimes M_n \cong \frac{\mathbb{Q}[s]}{(s^m)} \otimes \frac{\mathbb{Q}[t]}{(t^n)} \cong \frac{\mathbb{Q}[s,t]}{(s^m, t^n)},$$

which we identify with $\operatorname{span}_{\mathbb{Q}}\{s^i t^j \mid 0 \leq i < m, 0 \leq j < n\}$. $\mathbb{Z}$ acts on $M_m \otimes M_n$ via $\sigma = (1+s)(1+t) = 1+s+t+st$ and $\Delta = \sigma - 1 = s + t + st$.

We filter $M_m \otimes M_n$ by total degree writing $\mathcal{F}_r(M_m \otimes M_n) := \{h \in \mathbb{Q}[s,t]/(s^m, t^n) \mid \deg(h) \geq r\}$. For $h \in M_m \otimes M_n$, we write $\operatorname{gr}(h) = h_d$ where $h = h_d + h_{d+1} + \cdots + h_{m+n-2}$ with $h_d \neq 0$ and $h_r \in (M_m \otimes M_n)_r$. For $0 \neq h \in M_m \otimes M_n$, we define $\deg_*(h) = \deg(\operatorname{gr}(h))$. We consider the Hilbert function of $M_m \otimes M_n$ defined by

$$H(M_m \otimes M_n, j) := \dim (M_m \otimes M_n)_j$$

The Hilbert series of M_r is the polynomial $1 + \lambda + \lambda^2 + \cdots + \lambda^{r-1} = \frac{1-\lambda^r}{1-\lambda}$. Thus the Hilbert series of $M_m \otimes M_n$ is given by $\frac{1-\lambda^m}{1-\lambda}\frac{1-\lambda^n}{1-\lambda}$. Hence the Hilbert function of $M_m \otimes M_n$ is given by

$$H(M_m \otimes M_n, j) = \begin{cases} j+1 & \text{if } 0 \leq j \leq m-1, \\ m & \text{if } m-1 \leq j \leq n-1, \\ m+n-j-1 & \text{if } n-1 \leq j \leq n+m-2, \\ 0 & \text{otherwise.} \end{cases}$$

Proposition 9.2. *Let $1 \leq m \leq n$. For $r = 0, 1, \ldots, m-1$ there exists an element $\omega_r \in M_m(\mathbb{Z}) \otimes M_n(\mathbb{Z})$ such that $\Delta(\omega_r) = 0$ with $\deg_*(\omega_r) = m + n - r - 2$ and $\operatorname{gr}(\omega_r) = \sum_{i=0}^{r} (-1)^{i+1} s^{m-1-i} t^{n-r+i-1}$.*

Proof. We begin by showing that the homomorphism of $\mathbb{Z}$-modules

$$\Delta : \mathcal{F}_q(M_m(\mathbb{Z}) \otimes M_n(\mathbb{Z})) \to \mathcal{F}_{q+1}(M_m(\mathbb{Z}) \otimes M_n(\mathbb{Z}))$$

is surjective for all $q = n-1, n, \ldots, m+n-2$. We do this using downward induction on q. For $q = m+n-2$ the codomain $\mathcal{F}_{m+n-1}(M_m \otimes M_n)$ is 0 and so the result is trivially true.

Now suppose that $\Delta : \mathcal{F}_q(M_m(\mathbb{Z}) \otimes M_n(\mathbb{Z})) \to \mathcal{F}_{q+1}(M_m(\mathbb{Z}) \otimes M_n(\mathbb{Z}))$ is surjective and consider the map $\Delta : \mathcal{F}_{q-1}(M_m(\mathbb{Z}) \otimes M_n(\mathbb{Z})) \to \mathcal{F}_q(M_m(\mathbb{Z}) \otimes M_n(\mathbb{Z}))$. It is easy to verify that $(s+t)\sum_{k=0}^{m-i-1}(-1)^k s^{i+k} t^{q-i-k-1} = s^i t^{q-i}$ in $M_m \otimes M_n$ for

$q-n+1 \leq i \leq m-1$. Therefore $\operatorname{gr}(\Delta(\sum_{k=0}^{m-i-1}(-1)^k s^{i+k}t^{q-i-k-1})) = s^i t^{q-i}$. By the induction hypothesis,

$$\Delta(\mathcal{F}_{q-1}(M_m(\mathbb{Z})\otimes M_n(\mathbb{Z}))) \supseteq \Delta(\mathcal{F}_q(M_m(\mathbb{Z})\otimes M_n(\mathbb{Z}))) = \mathcal{F}_{q+1}(M_m(\mathbb{Z})\otimes M_n(\mathbb{Z})).$$

Furthermore,

$$\mathcal{F}_q(M_m(\mathbb{Z})\otimes M_n(\mathbb{Z})) = \Big(\bigoplus_{i=q-n+1}^{m-1} \mathbb{Z}s^i t^{q-i}\Big) \oplus \mathcal{F}_{q+1}(M_m(\mathbb{Z})\otimes M_n(\mathbb{Z})).$$

Thus $\Delta(\mathcal{F}_{q-1}(M_m(\mathbb{Z})\otimes M_n(\mathbb{Z}))) = \mathcal{F}_q(M_m(\mathbb{Z})\otimes M_n(\mathbb{Z}))$ as claimed.

Put $\omega_r' := \sum_{k=0}^{r}(-1)^k s^{m-r+k-1}t^{n-k-1} \in \mathcal{F}_{m+n-r-2}(M_m(\mathbb{Z})\otimes M_n(\mathbb{Z}))$. It is easy to check that $(s+t)\omega_r' = 0$ and thus $\deg_*(\Delta(\omega_r')) \geq \deg_*(\omega_r') + 2$. Thus we have $\Delta(\omega_r') \in \mathcal{F}_{m+n-r}(M_m(\mathbb{Z})\otimes M_n(\mathbb{Z}))$. By the above, there exists $\omega_r'' \in \mathcal{F}_{m+n-r-1}(M_m(\mathbb{Z})\otimes M_n(\mathbb{Z}))$ such that $\Delta(\omega_r'') = -\Delta(\omega_r')$. Taking $\omega_r := \omega_r' + \omega_r'' \in M_m(\mathbb{Z})\otimes M_n(\mathbb{Z})$ we have $\Delta(\omega_r) = 0$ with $\operatorname{gr}(\omega_r) = \omega_r'$ as required. □

Remark 9.3. Note that $M_q^{\mathbb{Z}} =$ (the kernel of $\Delta : M_q \to M_q$) is one-dimensional for all $q \geq n-1$. Since the direct sum decomposition of $M_m \otimes M_n$ into indecomposables has m summands, this implies that the kernel of $\Delta : M_m \otimes M_n \to M_m \otimes M_n$ has dimension m and thus $\{\omega_0, \omega_1, \ldots, \omega_{m-1}\}$ is a basis for this kernel. Furthermore, this kernel is contained in $\mathcal{F}_{n-1}(M_m \otimes M_n)$.

Theorem 9.4. *There exist elements $\alpha_0, \alpha_1, \ldots, \alpha_{m-1} \in M_m \otimes M_n$ such that for all $r = 0, 1, \ldots, m-1$ we have*

(1) $\deg_*(\Delta^j(\alpha_i)) = i + j$ *for all* $0 \leq i \leq r$ *and* $0 \leq j \leq m+n-2i-2$.
(2) $\{\operatorname{gr}(\Delta^j(\alpha_i)) \mid i \leq r,\ j \leq m+n-2i-2,\ i+j \leq r\}$ *is linearly independent.*
(3) $\{\Delta^j(\alpha_i) \mid 0 \leq i \leq r,\ m+n-i-r-2 \leq j \leq m+n-2i-2\}$ *is a basis for* $\mathcal{F}_{m+n-r-2}(M_m \otimes M_n)$.
(4) $\Delta^{m+n-2r-2}(\alpha_r) = \omega_r$ *and* $\ell(\omega_r) = m+n-2r-1$.

Proof. We proceed by complete induction on r. For $r = 0$ we take $\alpha_0 = 1/\binom{m+n-2}{m-1}$. Then $\Delta^{m+n-2}(\alpha_0) = s^{m-1}t^{n-1} = \omega_0$. Clearly this implies that $\ell(\omega_0) = m+n-1$. It is also clear that $\{\omega_0\}$ is a basis for the one-dimensional space $\mathcal{F}_{m+n-2}(M_m \otimes M_n)$. Since $\deg_*(\Delta^{m+n-2}(\alpha_0)) = m+n-2$ we must have $\deg_*(\Delta^j(\alpha_0)) = j$ for all $0 \leq j \leq m+n-2$. Finally, $\{\operatorname{gr}(\alpha_0)\} = \{\alpha_0\}$ is linearly independent.

Assume then that the four assertions hold for all values less than or equal to r and consider these four assertions for the value $r+1$. By the Clebsch–Gordan formula, $M_m \otimes M_n$ contains a summand isomorphic to $M_{m+n-2r-3}$. Thus there exists $\omega \in \ker\Delta$ with $\ell(\omega) = m+n-2r-3$. Take α such that $\Delta^{m+n-2r-4}(\alpha) = \omega$. Since $\ell(\omega_k) > m+n-2r-3$ for all $k \leq r$, we may write $\omega = \sum_{k=r+1}^{m-1} c_k\omega_k$ for some $c_k \in \mathbb{Q}$. Therefore $\deg_*(\omega) \leq \deg_*(\omega_{r+1}) = m+n-r-3$. This implies that $\deg_*(\alpha) \leq r+1$.

Combining (1) and (2) we see that $\{\operatorname{gr}(\Delta^j(\alpha_i)) \mid i \leq r,\ i+j \leq r\}$ is a basis for $\bigoplus_{d=0}^{r}(M_m \otimes M_n)_d$. Therefore we may write $\alpha = \sum_{i+j\leq r} a_{ij}\Delta^j(\alpha_i) + \alpha_{r+1}$ where $\alpha_{r+1} \in \mathcal{F}_{r+1}(M_m \otimes M_n)$ and $a_{ij} \in \mathbb{Q}$ for all i, j.

Now

$$0 = \Delta(\omega) = \Delta^{m+n-2r-3}(\alpha) = \sum_{i+j\le r} a_{ij}\Delta^{m+n-2r+j-3}(\alpha_i) + \Delta^{m+n-2r-3}(\alpha_{r+1}).$$

We consider this last expression in each degree $d = 0, 1, \ldots, m+n-r-3$. The component in degree d for $d = 0, 1, \ldots, m+n-2r-4$ is trivially 0. In degree $d = m+n-2r-3$ we find only $a_{00}\Delta^{m+n-2r-3}(\alpha_0)$ and thus $a_{00} = 0$. In degree $d = m+n-2r-2$ we find $a_{01}\Delta^{m+n-2r-3}(\alpha_1) + a_{10}\Delta^{m+n-2r-2}(\alpha_0)$. Therefore (using (3)) we have $a_{01} = a_{10} = 0$. Continuing in this manner up to degree $d = m+n-r-3$ we find that $a_{ij} = 0$ for all i, j. Therefore $\alpha = \alpha_{r+1}$ and $\deg_*(\alpha) \ge r+1$. We already observed that $\deg_*(\alpha) \le r+1$ and therefore $\deg_*(\alpha_{r+1}) = r+1$. Since $\deg_*(\Delta^{m+n-2r-4}(\alpha_{r+1})) = m+n-r-3$ we must have $\deg_*(\Delta^j(\alpha_{r+1})) = j+r+1$ for all $j = 0, 1, \ldots, m+n-2r-4$, which proves (1).

In particular, $\deg_*(\omega) \ge m+n-r-3$ and so we must have $\omega = c_{r+1}\omega_{r+1}$. Take $\alpha_{r+1} = c_{r+1}^{-1}\alpha$. Then $\Delta^{m+n-2r-4}(\alpha_{r+1}) = \omega_{r+1}$, which proves (4).

Now $\{\Delta^j(\alpha_i) \mid 0 \le i \le r+1,\ 0 \le j \le m+n-2i-2\}$ is a basis for $\bigoplus_{i=0}^{r+1} M_{m+n-2i-1}$ and so in particular is linearly independent. Counting dimensions implies that $\{\Delta^j(\alpha_i) \mid i+j \ge m+n-r-1,\ 0 \le i \le r+1,\ 0 \le j \le m+n-2i-2\}$ is a basis for $\mathcal{F}_{m+n-r-3}(M_m \otimes M_n)$, which proves (3).

Finally we prove (2). Assume there exists a linear relation

$$\sum_{i+j=d} b_{ij}\,\mathrm{gr}(\Delta^j(\alpha_i)) = 0$$

with scalars $b_{ij} \in \mathbb{Q}$ where $d \le r+1$. This linear relation (together with (1)) implies that

$$\sum_{i+j=d} b_{ij}\Delta^{m+n-r-d+j-3}(\alpha_i)) \in \mathcal{F}_{m+n-r-2}(M_m \otimes M_n)$$
$$= \mathrm{span}_{\mathbb{Q}}\{\Delta^k(\alpha_i) \mid 0 \le i \le r,\ i+k \ge m+n-r-2,\ k \le m+n-2k-2\}.$$

By (3) this means we may write

$$\sum_{i+j=d} b_{ij}\Delta^{m+n-r-d+j-3}(\alpha_i) = \sum_{i+j>m+n-3} b'_{ij}\Delta^j(\alpha_i).$$

But we have already seen that $\{\Delta^j(\alpha_i) \mid i+j \ge m+n-r-1,\ 0 \le i \le r+1,\ 0 \le j \le m+n-2i-2\}$ is linearly independent. Therefore each b_{ij} is 0, which proves (2). □

9.5. Decomposing $V_m \otimes V_n$

Next we want to determine an explicit decomposition of a tensor product of indecomposable C_p-modules, $V_m \otimes V_n$. Proposition 8.4 gives an abstract decomposition of $V_m \otimes V_n$. We want to obtain a more explicit description of this decomposition. To do this we consider the integer lattices $M_m(\mathbb{Z})$ and $M_n(\mathbb{Z})$ and the surjection $\rho : M_m(\mathbb{Z}) \otimes M_n(\mathbb{Z}) \to V_m \otimes V_n$ given by reduction modulo the prime p.

The following well-known result and its proof are included for the reader's convenience.

Lemma 9.6. *Let U be an n-dimensional $\mathbb{Q}$-vector space $U \cong \mathbb{Q}^n$ and suppose W is an r-dimensional subspace of U. Let $U(\mathbb{Z}) = \mathbb{Z}^n$ be the natural lattice in U. Let p be prime and let ρ denote the reduction modulo p map. Then $W(\mathbb{Z}) := W \cap U(\mathbb{Z})$ is a rank r lattice and $\rho(W(\mathbb{Z})) \cong \mathbb{F}_p^r$.*

Proof. The lattice $K_0 := pU(\mathbb{Z})$ is the kernel of the map ρ, and $W(\mathbb{Z}) \cap K_0$ is a free abelian group whose rank equals its minimal number of generators. Choose a vector space basis $\{v_1, \ldots, v_r\}$ of W. Scaling the v_i we may suppose that $v_i \in K_0$ and $u_i := (1/p)v_i \in U(\mathbb{Z}) \setminus K_0$. Thus $W(\mathbb{Z}) \cap K_0$ has rank at least r. If $W(\mathbb{Z}) \cap K_0$ required more than r generators we would find a relation among them from the $\mathbb{Q}$-linear dependence among them. Thus the rank of the lattice $W(\mathbb{Z}) \cap K_0$ is r and this lattice is generated by $v_1, \ldots, v_r$.

Furthermore $\{u_1, \ldots, u_r\}$ is a basis of $W(\mathbb{Z})$. To see this, take any $w \in W(\mathbb{Z})$. Then $pw \in W(\mathbb{Z}) \cap K_0$ and so we may write $pw = \sum_{i=1}^r c_i v_i$ where $c_i \in \mathbb{Z}$ for each i. Then $w = \sum_{i=1}^r c_i u_i$. This implies that the index of $W(\mathbb{Z}) \cap K_0$ in $W(\mathbb{Z})$ is p^r and $\rho(W(\mathbb{Z})) \cong W(\mathbb{Z})/(W(\mathbb{Z}) \cap K_0) \cong (\mathbb{Z}/p\mathbb{Z})^r$. □

Theorem 9.7. *Suppose $1 \le m \le n \le p$ with $m + n \ge p + 1$. Then $\ell(\rho(\omega_r)) = p$ for all $r = 0, 1, \ldots, m + n - p - 1$.*

Proof. By Proposition 8.4, the kernel of Δ on $V_m \otimes V_n$ is an m-dimensional $\mathbb{F}_p$-vector space. Since $\{\rho(\omega_0), \rho(\omega_1), \ldots, \rho(\omega_{m-1})\}$ is a linearly independent subset of $\ker \Delta$, it must be a basis for $\ker \Delta$. Thus

$$\begin{aligned}\Delta^{p-1}(V_m \otimes V_n) &\subseteq \ker \Delta \cap \mathcal{F}_{p-1}(V_m \otimes V_n)\\ &= \operatorname{span}_{\mathbb{F}_p}\{\rho(\omega_0), \rho(\omega_1), \ldots, \rho(\omega_{m-1})\} \cap \mathcal{F}_{p-1}(V_m \otimes V_n)\\ &= \operatorname{span}_{\mathbb{F}_p}\{\rho(\omega_0), \rho(\omega_1), \ldots, \rho(\omega_{m+n-p-1})\}.\end{aligned}$$

By Proposition 8.4, $\Delta^{p-1}(V_m \otimes V_n)$ has dimension $m + n - p$, which implies that the above inclusion is an equality. In particular $\ell(\rho(\omega_r)) = p$ for $r = 0, 1, \ldots, m+n-p-1$. □

Proposition 9.8. *There exist $\overline{\beta}_0, \overline{\beta}_1, \ldots, \overline{\beta}_{m+n-p-1} \in V_m \otimes V_n$ such that $\Delta^{p-1}(\overline{\beta}_r) = \rho(\omega_r)$ and $\deg_*(\overline{\beta}_r) = m + n - p - r - 1$ for $r = 0, 1, \ldots, m + n - p - 1$.*

Proof. By the above theorem there must exist $\overline{\beta'_0}, \overline{\beta'_1}, \ldots, \overline{\beta'_{m+n-p-1}} \in V_m \otimes V_n$ such that $\Delta^{p-1}(\overline{\beta'_r}) = \rho(\omega_r)$ for $r = 0, 1, \ldots, m+n-p-1$. Since $\deg_*(\rho(\omega_r)) = m+n-r-2$ we have $\deg_*(\overline{\beta'_r}) \le m+n-p-1-r$ for such r. This implies that $\deg_*(\overline{\beta'_{m+n-p-1}}) = 0$ and so we may take $\overline{\beta}_0 = \overline{\beta'_0}$.

Assume, by downward induction, that we have chosen $\overline{\beta}_i$ with $\Delta^{p-1}(\overline{\beta}_i) = \rho(\omega_i)$ and $\deg_*(\overline{\beta}_i) = m + n - p - i - 1$ for $i = r + 1, r + 2, \ldots, m + n - p - 1$ (where $r \ge 0$). The set

$$A_{r+1} := \{\Delta^j(\overline{\beta}_i) \mid r + 1 \le i \le m + n - p - 1,\ 0 \le j \le i - r - 1\}$$

is linearly independent and consists of elements x satisfying $\deg_*(x) \le r + 1$. Since the cardinality of A_{r+1} is

$$\sum_{i=r+1}^{m+n-p-1}(i-r)=\binom{m+n-p-1-r}{2}=\dim((V_m\otimes V_n)/\mathcal{F}_{m+n-p-r-1}(V_m\otimes V_n)),$$

the natural image of A_{r+1} forms a basis for $(V_m\otimes V_n)/\mathcal{F}_{m+n-p-r-1}(V_m\otimes V_n)$. Choose $\overline{\gamma}$ with $\deg_*(\overline{\gamma})=m+n-p-r-1$ such that the set $\{\overline{\gamma}\}\sqcup\{\Delta^j(\overline{\beta}_i)\mid r+1\le i\le m+n-p-1,\ 0\le j\le i-r\}$ similarly yields a basis for $(V_m\otimes V_n)/\mathcal{F}_{m+n-p-r}(V_m\otimes V_n)$. Write $\overline{\beta}'_r=c_0\overline{\gamma}+\sum_{i=r+1}^{m+n-p-1}\sum_{j=0}^{i-r}c_{ij}\Delta^j(\overline{\beta}_i)+\overline{\gamma'}$ where $c_0,c_{ij}\in\mathbb{F}_p$ and $\overline{\gamma'}\in\mathcal{F}_{m+n-p-r}(V_m\otimes V_n)$. Then

$$\rho(\omega_r)=\Delta^{p-1}(\overline{\beta}'_r)=\Delta^{p-1}(c_0\overline{\gamma})+\sum_{i=r+1}^{m+n-p-1}c_{i0}\rho(\omega_{m+n-p-i-1})+\Delta^{p-1}(\overline{\gamma'})$$

where $\deg_*(\Delta^{p-1}(\overline{\gamma'}))>\deg_*(\rho(\omega_{m+n-p-i-1}))$ for all $i\ge r+1$. Therefore $c_{i0}=0$ for all $i=r+1,r+2,\dots,m+n-p-1$ and $\rho(\omega_r)=\Delta^{p-1}(c_0\overline{\gamma}+\overline{\gamma'})$. Setting $\overline{\beta}_r=c_0\overline{\gamma}+\overline{\gamma'}$ yields $\deg_*(\overline{\beta}_r)=m+n-p-r-1$ and $\Delta^{p-1}(\overline{\beta}_r)=\rho(\omega_r)$ as required. □

We have seen that $M_m\otimes M_n\cong\bigoplus_{r=0}^{m-1}M_{m+n-2i-1}$ and that we may arrange this decomposition so that the socle of the summand $M_{m+n-2i+1}$ is spanned by ω_i. Furthermore α_i is a generator of the summand $M_{m+n-2i+1}$ with $\deg_*(\alpha_i)=i$ and $\Delta^{m+n-2i}(\alpha_i)=\omega_i$ for $i=0,1,\dots,m-1$. Moreover, by clearing denominators, we may assume that $\alpha_i\in(M_m\otimes M_n)(\mathbb{Z})$ with $\rho(\alpha_i)=a_i\omega_i\ne0$ for some $a_i\in\mathbb{Z}$.

Theorem 9.9. *Suppose $1\le m\le n\le p$ with $m+n\ge p+1$. For $m+n-p\le r\le m-1$, $\ell(\rho(\omega_r))=m+n-2r-1$. Furthermore,*

$$V_m\otimes V_n=\bigoplus_{r=m+n-p}^{m-1}V_{m+n-2r-1}\oplus(m+n-p)V_p$$

where

$$V_{m+n-2r-1}=\operatorname{span}_{\mathbb{F}_p}\{\Delta^j(\rho(\alpha_r))\mid 0\le j\le m+n-2r-2\}$$

for $m+n-p\le r\le m-1$. In particular

$$\rho(M_{m+n-2r-1}(\mathbb{Z}))=V_{m+n-2r-1}$$

for $m+n-p\le r\le m-1$ where $M_{m+n-2r-1}$ and $V_{m+n-2r-1}$ are indecomposable summands of $M_m\otimes M_n$ and $V_m\otimes V_n$ generated by α_r and $\rho(\alpha_r)$ respectively.

Proof. It suffices to show that $\Delta^{m+n-2r-2}(\rho(\alpha_r))\ne0$ for all $r\ge m+n-p$. Fix such an r. Let $\mathcal{K}M_r$ denote the kernel of $\Delta^{m+n-2r-2}:M_m\otimes M_n\to M_m\otimes M_n$. Then $\mathcal{K}M_r$ is a $\mathbb{Q}$-vector space and we write $\mathcal{K}M_r(\mathbb{Z}):=\mathcal{K}M_r\cap(M_m(\mathbb{Z})\otimes M_n(\mathbb{Z}))$. Observe that the set

$$\{\Delta^j(\alpha_i)\mid 0\le i\le r,\ 2r-2i+1\le j\le m+n-2i-2\}$$
$$\sqcup\{\Delta^j(\alpha_i)\mid r+1\le i\le m-1,\ 0\le j\le m+n-2i-2\}$$

is a basis for $\mathcal{K}M_r$. Either from this or by (9.1) we have

$$\begin{aligned}\dim_{\mathbb{Q}} \mathcal{K}M_r &= \sum_{i=0}^{r}(m+n-2r-2) + \sum_{i=r+1}^{m-1}(m+n-2i-1)\\ &= (r+1)(m+n-2r-2) + \sum_{i=r+1}^{m-1}(m+n-2i-1).\end{aligned}$$

Let $\mathcal{K}V_r$ denote the kernel of $\Delta^{m+n-2r-2} : V_m \otimes V_n \to V_m \otimes V_n$. By Proposition 8.4, we see that $\dim_{\mathbb{F}_p} \mathcal{K}V_r = (r+1)(m+n-2r-2) + \sum_{i=r+1}^{m-1}(m+n-2i-1) = \dim_{\mathbb{Q}} \mathcal{K}M_r$. Therefore, applying Lemma 9.6, we see that $\rho(\mathcal{K}M_r(\mathbb{Z})) = \mathcal{K}V_r$. Since $\alpha_r \notin \mathcal{K}M_r$, this implies that $\rho(\alpha_r) \notin \mathcal{K}M_r$, i.e., $\Delta^{m+n-2r-2}(\rho(\alpha_r)) \neq 0$ as required. Thus $\Delta^{m+n-2r-2}(\rho(\alpha_r))$ is a non-zero multiple of $\rho(\omega_r)$ and so $\ell(\rho(\omega_r)) \geq m+n-2r-1$. Since this is true for all $r = m+n-p, m+n-p+1, \ldots, m-1$, comparing with Proposition 8.4 shows that $\ell(\rho(\omega_r)) = m+n-2r-1$ as required. □

Remark 9.10. Since $\rho(\Delta^{m+n-2r-2}(\alpha_r)) \neq 0$ we may replace α_r by an integer multiple of itself in order to arrange that $\Delta^{m+n-2r-2}(\rho(\alpha_r)) = \rho(\omega_r)$ for $r = m+n-p$, $m+n-p+2, \ldots, m-1$.

Remark 9.11. One component of our proofs of Theorems 9.4 and 9.9 involves showing that the multiplication maps

$$(s+t)^{m+n-2r-2}\cdot : (M_m \otimes M_n)_r \to (M_m \otimes M_n)_{m+n-r-2}$$

for $r = 0, 1, \ldots, m-1$ and

$$(s+t)^{m+n-2r-2}\cdot : (V_m \otimes V_n)_r \to (V_m \otimes V_n)_{m+n-r-2}$$

for $r = m+n-p, m+n-p+1, \ldots, m-1$ are surjective. Another way to show this is to consider the matrix associated to these maps with respect to the basis of monomials in s and t. This matrix is given by

$$D_{r+1}(m+n-2r-2, m-r-1) := \left(\binom{m+n-2r-2}{m-r-1+i-j}\right)_{\substack{1\leq i\leq r+1\\ 1\leq j\leq r+1}}.$$

Srinivasan [44] shows that this matrix is row equivalent to her *Pascal matrix*

$$P_{r+1,r+1}(m+n-2r-2, m-r-1) := \left(\binom{m+n-2r-3+i}{m-r-2+j}\right)_{\substack{1\leq i\leq r+1\\ 1\leq j\leq r+1}}.$$

Moreover this row equivalence may be obtained using only determinant preserving row operations. Srinivasan shows that this latter matrix has determinant

$$\frac{1!\,2!\cdots r!}{(m-r)^r(m-r+1)^{r-1}\cdots(m-1)}\prod_{c=0}^{r}\binom{m+n-2r-2+c}{m-r-1}.$$

This determinant is always non-zero, and is non-zero modulo p if and only if $m+n-r-2 < p$.

Theorem 9.12. *Suppose* $1 \le m_i \le p$ *for* $i = 1, \dots, r$. *Write* $V_{n_1} \otimes \cdots \otimes V_{n_r} \cong \bigoplus_{i=1}^{p} a_i V_i$. *Then* $M_{n_1} \otimes \cdots \otimes M_{n_r}$ *contains a summand* N *with* $N \cong \bigoplus_{i=1}^{p-1} a_i M_i$ *such that* $\rho(N(\mathbb{Z})) = W$ *where* W *is a summand of* $\bigotimes_{k=1}^{n-1} V_{n_k}$ *with* $W \cong \bigoplus_{i=1}^{p-1} a_i V_i$. *More explicitly, we may decompose* N *and* W *into indecomposable summands,* $N = \bigoplus_{\alpha\in\Gamma} N_\alpha$ *and* $W = \bigoplus_{\alpha\in\Gamma} W_\alpha$, *with* $\dim_{\mathbb{Q}} M_\alpha = \dim_{\mathbb{F}_p} W_\alpha$ *and* $\rho(M_\alpha(\mathbb{Z})) = W_\alpha$ *for all* $\alpha \in \Gamma$.

Proof. The proof is by induction on r. The result is trivial for $r = 1$.

Decompose $\bigotimes_{k=1}^{r-1} V_{n_k}$ into a direct sum of indecomposables C_p-modules:

$$V_{n_1} \otimes \cdots \otimes V_{n_{r-1}} = \bigoplus_{\alpha\in A} W_\alpha.$$

Define $A' := \{\alpha \in A \mid \dim W_\alpha < p\}$ and $A'' := A \setminus A' = \{\alpha \in A \mid \dim W_\alpha = p\}$. Define $W' := \bigoplus_{\alpha\in A'} W_\alpha$ and $W'' := \bigoplus_{\alpha\in A''} W_\alpha$ so that $\bigotimes_{k=1}^{r-1} V_{n_k} = W' \oplus W''$.

By induction $M_{n_1} \otimes \cdots \otimes M_{n_{r-1}}$ contains a summand U' with $U' = \bigoplus_{\alpha\in A'} N_\alpha$ where $N_\alpha \cong M_{\theta(\alpha)}$ with $\theta(\alpha) = \dim_{\mathbb{Q}} N_\alpha = \dim_{\mathbb{F}_p} W_\alpha < p$ and $\rho(N_\alpha(\mathbb{Z})) = W_\alpha$ for all $\alpha \in A'$. Thus $\rho(U'(\mathbb{Z})) = W'$.

Decompose $W_\alpha \otimes V_{n_r} = \bigoplus_{\beta\in B_\alpha} W_{\alpha,\beta}$ and define $B'_\alpha := \{\beta \in B_\alpha \mid \dim W_{\alpha,\beta} < p\}$ and $B''_\alpha := B_\alpha \setminus B'_\alpha$. By Theorem 9.9 and Remark 9.10, $M_\alpha \otimes M_{n_r}$ contains a summand $\bigoplus_{\beta\in B'_\alpha} N_{\alpha,\beta}$ with $N_{\alpha,\beta} \cong M_{\theta(\beta)}$ where $\theta(\beta) = \dim_{\mathbb{Q}} N_{\alpha,\beta} = \dim_{\mathbb{F}_p} W_{\alpha,\beta} < p$ and $\rho(N_{\alpha,\beta}(\mathbb{Z})) = W_{\alpha,\beta}$ for all $\beta \in B'_\alpha$ and all $\alpha \in A'$. Thus we have

$$\begin{aligned}
\bigotimes_{k=1}^{r} V_{n_k} &\cong (W' \otimes V_{n_r}) \oplus (W'' \otimes V_{n_r}) = \Big(\bigoplus_{\alpha\in A'} W_\alpha \otimes V_{n_r}\Big) \oplus (W'' \otimes V_{n_r}) \\
&= \Big(\bigoplus_{\alpha\in A'} \bigoplus_{\beta\in B_\alpha} W_{\alpha,\beta}\Big) \oplus (W'' \otimes V_{n_r}) \\
&= \Big(\bigoplus_{\alpha\in A'} \bigoplus_{\beta\in B'_\alpha} W_{\alpha,\beta}\Big) \oplus \Big(\bigoplus_{\alpha\in A'} \bigoplus_{\beta\in B''_\alpha} W_{\alpha,\beta}\Big) \oplus (W'' \otimes V_{n_r})
\end{aligned}$$

where $(\bigoplus_{\alpha\in A'} \bigoplus_{\beta\in B''_\alpha} W_{\alpha,\beta}) \oplus (W'' \otimes V_{n_r})$ is a free C_p-module and $W \cong \bigoplus_{\alpha\in A'} \bigoplus_{\beta\in B'_\alpha} W_{\alpha,\beta}$.

Taking N to be the summand $N := \bigoplus_{\alpha\in A'} \bigoplus_{\beta\in B'_\alpha} N_{\alpha,\beta}$ of $\bigotimes_{k=1}^{r} M_{n_k}$ we have $\rho(N_{\alpha,\beta}(\mathbb{Z})) = W_{\alpha,\beta}$ for all $\alpha \in A'$ and all $\beta \in B'_\alpha$ and $\rho(N(\mathbb{Z})) = W$ as required. □

Corollary 9.13. *Suppose* $1 \le n_1, \dots, n_k \le p$. *Every invariant* $f \in (\bigotimes_{k=1}^{r} V_{n_k})^{C_p}$ *may be expressed as a sum* $f = f_0 + f_1$ *where* f_0 *is integral (i.e.,* $f_0 = \rho(F_0)$ *for some* $F_0 \in (\bigotimes_{k=1}^{r} M_{n_k}(\mathbb{Z}))^{\mathbb{Z}}$*) and* f_1 *is a transfer.*

We now apply this to symmetric algebras.

Theorem 9.14. *Let* $1 < n_1, \dots, n_r \le p$ *and* $0 \le d_1, \dots, d_r \le p-1$. *Every invariant* $f \in \mathbb{F}_p[V_{n_1} \oplus \cdots \oplus V_{n_r}]^{C_p}_{(d_1,\dots,d_r)}$ *may be written as* $f' + f''$ *where* f' *is integral and* f'' *is a transfer, i.e.,* $f' = \rho(F')$ *for some* $F' \in \mathbb{Z}[M_{n_1} \oplus \cdots \oplus M_{n_r}]^{\mathbb{Z}}_{(d_1,\dots,d_r)}$ *and* $f'' = \mathrm{Tr}^{C_p}(F'')$ *for some* $F'' \in \mathbb{F}_p[V_{n_1} \oplus \cdots \oplus V_{n_r}]_{(d_1,\dots,d_r)}$.

Proof. Let $d < p$. The symmetric group on d letters, Σ_d, acts on $\bigotimes^d V_n^*$ by permuting factors. Furthermore $\mathrm{Sym}^d V_n^* = (\bigotimes^d V_n^*)^{\Sigma_d}$. Since $d < p$, the group Σ_d is non-modular and therefore $\mathrm{Sym}^d V_n^*$ has a Σ_d-stable complement: $\bigotimes^d V_n^* = \mathrm{Sym}^d V_n^* \oplus U$. Since the actions of C_p (in fact all of $\mathrm{GL}(V_n^*)$) and Σ_d commute, the complement U is also a C_p-module (in fact a $\mathrm{GL}(V_n^*)$-module). Therefore $\mathrm{Sym}^d V_n^*$ is a summand of $\bigotimes^d V_n^*$ as a C_p-module.

Similarly $\mathrm{Sym}^d M_n^*$ is a summand of the $\mathbb{Z}$-module $\bigotimes^d M_n^*$. The projection of $\bigotimes^d V_n^*$ onto $\mathrm{Sym}^d V_n^*$ is given by the Reynolds operator $\Pi_{\Sigma_d} = (1/d!)\sum_{\tau\in\Sigma_d}\tau$. The same formula gives the projection of $\bigotimes^d M_n^*$ onto $\mathrm{Sym}^d M_n^*$.

In the same manner, $\mathbb{F}_p[V_{n_1}\oplus\cdots\oplus V_{n_r}]_{(d_1,\dots,d_r)} = \mathrm{Sym}^{d_1} V_{n_1}^* \otimes\cdots\otimes \mathrm{Sym}^{d_r} V_{n_r}^*$ is a summand of the C_p-module $\bigotimes_{i=1}^r \bigotimes^{d_i} V_{n_i}^*$, and $\mathbb{Q}[M_{n_1}\oplus\cdots\oplus M_{n_r}]_{(d_1,\dots,d_r)} = \mathrm{Sym}^{d_1} M_{n_1}^* \otimes\cdots\otimes \mathrm{Sym}^{d_r} M_{n_r}^*$ is a summand of the $\mathbb{Z}$-module $\bigotimes_{i=1}^r \bigotimes^{d_i} M_{n_i}^*$. The projection onto these summands is given by the Reynolds operator Π associated to the Young subgroup $\Sigma_{d_1,\dots,d_r} := \Sigma_{d_1}\times\cdots\times\Sigma_{d_r}$ where

$$\Pi = \Pi_{\Sigma_{d_1,\dots,d_r}} = \frac{1}{d_1!\cdots d_r!}\sum_{\tau\in\Sigma_{d_1,\dots,d_r}}\tau.$$

By Corollary 9.13, every invariant $f\in\mathbb{F}_p[V_{n_1}\oplus\cdots\oplus V_{n_r}]^{C_p}_{(d_1,\dots,d_r)}$ can be written as a sum $f = f_0 + f_1$ where $f_0 = \rho(F_0)$ for some $F_0\in(\bigotimes_{j=1}^r\bigotimes^{d_j} M_{n_j}^*(\mathbb{Z}))^{\mathbb{Z}}$ and $f_1 = \mathrm{Tr}^{C_p}(F_1)$ for some $F_1\in\bigotimes_{j=1}^r\bigotimes^{d_j} V_{n_j}^*$. Therefore

$$f = \Pi(f) = \Pi(f_0+f_1) = \Pi(f_0)+\Pi(f_1) = \Pi(\rho(F_0))+\Pi(\mathrm{Tr}^{C_p}(F_1)).$$

Clearly $\Pi(\rho(F_0)) = \rho(\Pi(F_0))$. Since the actions of $\Sigma_{d_1,\dots,d_r}$ and of C_p on $\bigotimes_{i=1}^r\bigotimes^{d_i} V_{n_i}^*$ commute, we have $\Pi(\mathrm{Tr}^{C_p}(F_1)) = \mathrm{Tr}^{C_p}(\Pi(F_1))$. Similarly the actions of $\Sigma_{d_1,\dots,d_r}$ and of $\mathbb{Z}$ on $\bigotimes_{i=1}^r\bigotimes^{d_i} M_{n_i}^*$ commute and thus $\Pi(F_0)$ is a $\mathbb{Z}$-invariant since F_0 is. Therefore $f = \rho(\Pi(F_0))+\mathrm{Tr}^{C_p}(\Pi(F_1))$ where $\Pi(F_0)\in\mathbb{Q}[M_{n_1}\oplus\cdots\oplus M_{n_r}]^{\mathbb{Z}}_{(d_1,\dots,d_r)}$ and $\Pi(F_1)\in\mathbb{F}_p[V_{n_1}\oplus\cdots\oplus V_{n_r}]_{(d_1,\dots,d_r)}$. Hence we have written f as the sum of an integral invariant and a transfer.

Also note that Roberts' isomorphism implies that $\Pi(F_0) = \psi(h)$ for some $h\in\mathbb{C}[R_1\oplus R_{n_1-1}\oplus\cdots\oplus R_{n_r-1}]^{\mathrm{SL}_2(\mathbb{C})}$. □

Combining Therem 9.14 with the Periodicity Theorem we have a proof of the conjecture:

Theorem 9.15. *Let $V = \bigoplus_{i=1}^r V_{n_i}$. For each $i = 1,\dots,r$, choose a generator z_i of the cyclic module C_p-module $V_{n_i}^*$, i.e., choose $z_i\in V_{n_i}^*\setminus\Delta(V_{n_i}^*)$. Put $N_i := N^{C_p}(z_i)$. Then $\mathbb{F}_p[V]^{C_p}$ is generated by $N_1,\dots,N_r$ together with a finite set of integral invariants and a finite set of transfer invariants.*

Proof. Given $f\in\mathbb{F}_p[V]^{C_p}$ we may use the decomposition from the Periodicity Theorem to write $f = f^\sharp + f^\flat$ with $f^\sharp = \sum_{i=1}^r f_i N_i$ where each f_i is in $\mathbb{F}_p[V]^{C_p}$ and $f^\flat\in(\mathbb{F}_p[V]^{C_p})^\flat$. Thus we may choose a generating set for $\mathbb{F}_p[V]^{C_p}$ consisting of elements of

$(\mathbb{F}_p[V]^{C_p})^\flat$ together with the r norms $N_1, \ldots, N_r$. Of course, we can and will choose the elements $(\mathbb{F}_p[V]^{C_p})^\flat$ to be multi-graded. Given such a generator $f \in (\mathbb{F}_p[V]^{C_p}_{(d_1,\ldots,d_r)})^\flat$ we see by the Periodicity Theorem that if there exists an i with $d_i > p-n_i$ then $\ell(f) = p$, i.e., $f = \Delta^{p-1}(F)$ for some $F \in \mathbb{F}_p[V]^\flat$. Since $\Delta^{p-1}(F) = (\sigma - 1)^{p-1}(F) = (1 + \sigma + \sigma^2 + \cdots + \sigma^{p-1})(F) = \mathrm{Tr}(F)$, we see that $d_i > p - n_i$ forces f to be in the image of the transfer. Note that the degree conditions $d_i \leq p - n_i$ ensure that the vector space spanned by the integral non-transfer invariants is finite-dimensional.

Following [40, Theorem 6.2], we see that there is a homogeneous system of parameters for $\mathbb{F}_p[V]^{C_p}$ consisting of $N_1, \ldots, N_r$ together with a number of transfers of degree $p - 1$. Let A denote the polynomial algebra generated by this homogeneous system of parameters. Since $\mathbb{F}_p[V]$ is Cohen–Macaulay we have the Hironaka decomposition

$$\mathbb{F}_p[V] = \bigoplus_{k=1}^{q} Ah_k$$

where $h_k \in \mathbb{F}_p[V]$ for all k. Since the transfer is an A-module map, $\{\mathrm{Tr}(h_k) \mid k = 1, \ldots, q\}$ forms a set of A-module generators for the ideal $\mathrm{Tr}(\mathbb{F}_p[V])$. These q transfers together with the $\dim V$ many elements in the homogeneous system of parameters and the finitely many integral non-transfer invariants form a finite algebra generating set for $\mathbb{F}_p[V]^{C_p}$. □

The following more explicit formulation of the above theorem is useful.

Corollary 9.16. *Let $V = \bigoplus_{i=1}^{r} V_{n_i}$. For each $i = 1, \ldots, r$, choose a generator z_i of the cyclic module C_p-module $V_{n_i}^*$, i.e., choose $z_i \in V_{n_i}^* \setminus \Delta(V_{n_i}^*)$. Put $N_i := N^{C_p}(z_i)$ and $z_{ij} = \Delta^j(z_i)$ for all $1 \leq i \leq r$ and $0 \leq j \leq n_i - 1$. Suppose there exist invariants $f_{ij} \in \mathbb{F}[V]^G$ and positive integers d_{ij} such $\mathrm{LT}(f_{ij}) = z_{ij}^{d_{ij}}$ for all $1 \leq i \leq r$ and $1 \leq j \leq n_i - 1$. Put $d_{0j} = p$ (since $\mathrm{LT}(N_i) = z_i^p$). Then $\mathbb{F}_p[V]^{C_p}$ is generated by the following invariants:*

- $N_1, \ldots, N_r$;
- f_{ij} *with* $1 \leq i \leq r$ *and* $1 \leq j \leq n_i - 1$;
- *a finite set of integral invariants;*
- $\mathrm{Tr}(\prod_{i=1}^{r} \prod_{j=0}^{n_i-1} z_{ij}^{a_{ij}})$ *with* $0 \leq a_{ij} < d_{ij}$ *for all* $1 \leq i \leq r$ *and* $1 \leq j \leq n_i - 1$.

Proof. The hypotheses imply (by [20, Lemma 6.2.1]) that the set

$$\{N_1, \ldots, N_r\} \cup \{f_{ij} \mid 1 \leq i \leq r,\ 1 \leq j \leq n_i - 1\}$$

forms a homogeneous system of parameters. Let A denote the polynomial algebra generated by these $\dim V$ many invariants. By Theorem 9.15, $\mathbb{F}_p[V]^{C_p}$ is generated by A together with a finite set of integral invariants and some transfers. Consider the set of monomials $\Gamma = \{\prod_{i=1}^{r} \prod_{j=0}^{n_i-1} z_{ij}^{a_{ij}} \mid 0 \leq a_{ij} < d_{ij}\}$. Then

$$\mathbb{F}_p[V] = \bigoplus_{\gamma \in \Gamma} A\gamma.$$

Thus $\{\mathrm{Tr}(\gamma) \mid \gamma \in \Gamma\}$ is a set of A-module generators for the ideal $\mathrm{Tr}(\mathbb{F}[V])$. □

10. Applications

We use Corollary 9.16 to give generators for the invariant ring of a number of representations of C_p.

10.1. The invariant ring $\mathbb{F}[V_2 \oplus V_4]^{C_p}$

We mentioned in the introduction that the C_p-representation $V_2 \oplus V_4$ is the only remaining reduced representation whose ring of invariants is likely to be computable by the SAGBI basis method originally developed by Shank. Here we will find generators for this ring much more easily by using the proof of the conjecture.

We need to find the ring of covariants of $R_1 \oplus R_3$. A method to find generators for this ring is given in [29, §138A]. Letting L denote the linear form and f the cubic form we have the following 13 generators for this ring of covariants.

Table 1. Covariants of $R_1 \oplus R_3$

Covariant	Order	Bi-degree	LM	LM(Source)
L	1	$(1, 0)$	a_0x	x_1
f	3	$(0, 1)$	b_0x^3	x_2
$H := (f, f)^2$	2	$(0, 2)$	$b_1^2x^2$	y_2^2
$T := (f, H)^1$	3	$(0, 3)$	$b_1^3x^3$	y_2^3
$\Delta := (H, H)^2$	0	$(0, 4)$	$b_1^3b_3$	$y_2^2z_2^2$
$(f, L)^1$	2	$(1, 1)$	$a_1b_0x^2$	x_1y_2
$(f, L^2)^2$	1	$(2, 1)$	$a_1^2b_0x$	$x_1^2z_2$
$(f, L^3)^3$	0	$(3, 1)$	$a_1^3b_0$	$x_1^3w_2$
$(H, L)^1$	1	$(1, 2)$	$a_1b_1^2x$	$x_1y_2z_2$
$(H, L^2)^2$	0	$(2, 2)$	$a_1^2b_1^2$	$x_1^2z_2^2$
$(T, L)^1$	2	$(1, 3)$	$a_1b_1^3x^2$	$x_1y_2^2z_2$
$(T, L^2)^2$	1	$(2, 3)$	$a_1^2b_1^3x$	$x_1^2y_2z_2^2$
$(T, L^3)^3$	0	$(3, 3)$	$a_1^3b_1^3$	$x_1^3z_2^3$

Here we are using $\{x, y\}$ as a basis for the dual of the first copy of R_1, $\{a_0, a_1\}$ as a basis for the dual of the second copy of R_1, and $\{b_0, 3b_1, 3b_2, b_3\}$ as the basis for R_3^*. Thus $L = a_0x + a_1y$ and $f = b_0x^3 + 3b_1x^2y + 3b_2xy^2 + b_3y^3$. As in Section 4, these bases are chosen so that both L and f are invariant. In the column labelled "LM" we give the lead monomial of the covariant and in the final column we give the lead monomial of the corresponding source.

Examining these lead terms we easily see that no one of these 13 covariants can be written as a polynomial in the other 12. Thus these 13 covariants minimally generate $\mathbb{C}[R_1 \oplus R_1 \oplus R_3]^{\mathrm{SL}_2(\mathbb{C})}$. Applying Roberts' isomorphism and reducing modulo p yields

13 integral invariants in $\mathbb{F}[V_2 \oplus V_4]^{C_p}$. Here $\{x_1, y_1\}$ is a basis of V_2^* and $\{x_2, y_2, z_2, w_2\}$ is a basis of V_4^*. We use the graded reverse lexicographic ordering with $w_2 > z_2 > y_2 > y_1 > x_2 > x_1$. The lead terms of these 13 C_p-invariants are given in the final column of Table 10.1. We have integral invariants with lead terms x_1, x_2 and y_2^2. The lead monomial of $\mathrm{Tr}(w_2^{p-1})$ is z_2^{p-1}. Thus $\mathbb{F}[V_2 \oplus V_4]^{C_p}$ is generated by 13 integral invariants, the two norms $N^{C_p}(y_1)$, $N^{C_p}(w_2)$, and the family of transfers $\mathrm{Tr}(w_2^{d_2} z_2^{c_2} y_2^{b_2} y_1^{b_1})$ with $0 \le d_2 \le p-1, 0 \le c_2 \le p-2, 0 \le b_2 \le 1, 0 \le b_1 \le p-1$.

10.2. The invariant ring $\mathbb{F}[V_3 \oplus V_4]^{C_p}$

Here we complete the computations discussed in Examples 4.1 and 7.1 by finding generators for $\mathbb{F}[V_3 \oplus V_4]^{C_p}$. Let $\phi = a_0x^2 + 2a_1xy + a_2y^2$ and $f = b_0x^3 + 3b_1x^2y + 3b_2xy^2 + b_3y^3$ denote the quadratic and cubic forms respectively. Here we are using $\{x, y\}$ as a basis for R_1^*, $\{a_0, 2a_1, a_2\}$ as a basis for R_2^*, and $\{b_0, 3b_1, 3b_2, b_3\}$ as a basis for R_3^*. As in Section 4, these bases are chosen so that both ϕ and f are invariant. In the column labelled "LM" we give the lead monomial of the covariant.

Generators for the ring of covariants $\mathbb{C}[R_1 \oplus R_2 \oplus R_3]^{\mathrm{SL}_2(\mathbb{C})}$ are given in [29, §140]. There are 15 generators as follows:

Table 2. Covariants of $R_2 \oplus R_3$

Covariant	Order	Bi-degree	LM	LM(Source)
ϕ	2	(1, 0)	a_0x^2	x_1
f	3	(0, 1)	b_0x^3	x_2
$H := (f, f)^2$	2	(0, 2)	$b_1^2x^2$	y_2^2
$T := (f, H)^1$	3	(0, 3)	$b_1^3x^3$	y_2^3
$\Delta := (H, H)^2$	0	(0, 4)	$b_1^2b_2^2$	$y_2^2z_2^2$
$D := (\phi, \phi)^2$	0	(2, 0)	a_1^2	y_1^2
(ϕ, f)	3	(1, 1)	$a_1b_0x^3$	x_1y_2
$(\phi, f)^2$	1	(1, 1)	a_2b_0x	x_1z_2
$(\phi^2, f)^3$	1	(2, 1)	$a_1a_2b_0x$	$x_1^2w_2$
$(\phi^3, f^2)^6$	0	(3, 2)	$a_2^3b_0^2$	$x_1^3w_2^2$
(ϕ, H)	2	(1, 2)	$a_1b_1^2x^2$	$x_1y_2z_2$
$(\phi, H)^2$	0	(1, 2)	$a_2b_1^2$	$x_1z_2^2$
$(\phi, T)^2$	1	(1, 3)	$a_2b_1^3x$	$x_1y_2z_2^2$
$(\phi^2, T)^3$	1	(2, 3)	$a_1a_2b_1^3x$	$x_1^2z_2^3$
$(\phi^3, fT)^6$	0	(3, 4)	$a_2^3b_0b_1^3$	$x_1^3z_2^3w_2$

Examining their lead terms we see that these 15 covariants minimally generate the ring $\mathbb{C}[R_1 \oplus R_2 \oplus R_3]^{\mathrm{SL}_2(\mathbb{C})}$. Applying Roberts' isomorphism and reducing modulo p

yields 15 integral invariants in $\mathbb{F}[V_3 \oplus V_4]^{C_p}$. Here $\{x_1, y_1, z_1\}$ is a basis of V_3^* and $\{x_2, y_2, z_2, w_2\}$ is a basis of V_4^*. We use the graded reverse lexicographic order with $w_2 > z_2 > z_1 > y_2 > y_1 > x_2 > x_1$. The lead terms of these 15 C_p-invariants are given in the final column of Table 10.2. We have integral invariants with lead terms x_1, x_2, y_1^2 and y_2^2. Since $\mathrm{LM}(\mathrm{Tr}(w_2^{p-1})) = z_2^{p-1}$ we see by Corollary 9.16 that $\mathbb{F}[V_3 \oplus V_4]^{C_p}$ is generated by the 15 integral invariants, the two norms $N^{C_p}(z_1)$, $N^{C_p}(w_2)$ and the family of transfers $\mathrm{Tr}(w_2^{d_2} z_2^{c_2} y_2^{b_2} z_1^{c_1} y_1^{b_1})$ with $0 \le d_2 \le p-1$, $0 \le c_2 \le p-2$, $0 \le b_2 \le 1$, $0 \le c_1 \le p-1$ and $0 \le b_1 \le 2$.

10.3. Vector invariants of V_2

Here we take an arbitrary positive integer m and find generators for $\mathbb{F}_p[mV_2]^{C_p}$. Suppose the dual of the i^{th} copy of V_2 is spanned by $\{x_i, y_i\}$ where $\Delta(y_i) = x_i$ and $\Delta(x_i) = 0$. As discussed in the introduction, this ring of invariants was first computed by Campbell and Hughes [18]. Recently Campbell, Shank and Wehlau [19] gave a simplified proof. Here we give a shorter proof. Importantly, the proof in [19] yields the stronger and computationally very useful result that the minimal generating set for $\mathbb{F}_p[mV_2]^{C_p}$ is also a SAGBI basis with respect to a certain term order.

The integral invariants $\mathbb{F}_p[mV_2]^{C_p}$ lift via the Roberts' isomorphism to invariants of $\mathbb{C}[(m+1)R_1]^{\mathrm{SL}_2(\mathbb{C})}$. By the first fundamental theorem for $\mathrm{SL}_2(\mathbb{C})$ (see [35, §11.1.2, Theorem 1] for example), this ring is generated by $\binom{m+1}{2}$ quadradic determinants $U_{i,j}$ with $0 \le i < j \le m$. Applying Roberts' isomorphism (and reducing modulo p) yields the integral invariants $u_{0j} = x_j$ for $j = 1, \ldots, m$ and $u_{i,j} = x_i y_j - x_j y_i$ for $1 \le i < j \le m$. Thus applying Corollary 9.16 we see that $\mathbb{F}_p[mV_2]^{C_p}$ is generated by

- x_j for $j = 1, \ldots, m$;
- $N^{C_p}(y_i) = y_i^p - x_i^{p-1} y_i$ for $i = 1, \ldots, m$;
- $u_{i,j} = x_i y_j - x_j y_i$ for $1 \le i < j \le m$;
- $\mathrm{Tr}(y_1^{a_1} \cdots y_m^{a_m})$ where $0 \le a_1, \ldots, a_m < p$.

This set is not a minimal generating set. Shank and Wehlau [43] showed that it becomes a minimal generating set if all the transfers of degree less than $2p-1$ are omitted.

10.4. Vector invariants of V_3

Here we take an arbitrary positive integer m and find generators for $\mathbb{F}_p[mV_3]^{C_p}$. This is the first computation of this ring of invariants. It is possible to adapt the technique used in [19] to give a SAGBI basis for $\mathbb{F}_p[mV_3]^{C_p}$ (cf. [46]).

Suppose the dual of the i^{th} copy of V_3 is spanned by $\{x_i, y_i, z_i\}$ where $\Delta(z_i) = y_i$, $\Delta(y_i) = x_i$ and $\Delta(x_i) = 0$.

The integral invariants here lift via Roberts' isomorphism to invariants of the ring $\mathbb{C}[R_1 \oplus mR_2]^{\mathrm{SL}_2(\mathbb{C})}$, i.e., to covariants of mR_2.

Generators for this ring were found classically. See for example [29, §139A]. This ring is generated by the $\binom{m+1}{2}$ quadradic determinants $U_{i,j} = (\phi_i, \phi_j)^1$ with $0 \le i < j \le m$

together with $\binom{m+1}{2}$ further quadratic polynomials $D_{i,j} = (\phi_i, \phi_j)^2$ with $1 \le i \le j \le m$ and $\binom{m}{3}$ determinant invariants $\mathrm{Det}_{i,j,k}$ with $1 \le i < j < k \le m$. Applying Roberts' isomorphism we get

$$\begin{aligned}
\psi(U_{i,j}) &= u_{i,j} = x_i y_j - x_j y_i \quad \text{if } i \neq 0,\\
\psi(U_{0,j}) &= x_j,\\
\psi(D_{i,j}) &= d_{i,j} = 2y_i y_j - 2z_i x_j - 2x_i z_j - x_i y_j - y_i x_j,\\
\psi(\mathrm{Det}_{i,j,k}) &= \det_{i,j,k} = x_i y_j z_k - x_i z_j y_k + z_i x_j y_k - y_i x_j z_k + y_i z_j x_k - z_i y_j x_k.
\end{aligned}$$

Since $\mathrm{LM}(d_{i,i}) = y_i^2$ we have the following theorem.

Theorem 10.5. *$\mathbb{F}_p[mV_3]^{C_p}$ is generated by*

- *$N^{C_p}(z_i)$ for $i = 1, \dots, m$;*
- *x_i for $i = 1, \dots, m$;*
- *$u_{i,j}$ with $1 \le i < j \le m$;*
- *$d_{i,j}$ with $1 \le i \le j \le m$;*
- *$\det_{i,j,k}$ with $1 \le i < j < j \le m$;*
- *$\mathrm{Tr}(\prod_{i=1}^m y_i^{b_i} z_i^{c_i})$ with $0 \le b_i \le 1$ and $0 \le c_i \le p-1$.*

10.6. Vector invariants of V_4

Here we give generators for $\mathbb{F}_p[mV_4]^{C_p}$. This is the first computation of this ring of invariants. Suppose the dual of the i^{th} copy of V_4 is spanned by $\{x_i, y_i, z_i, w_i\}$ where $\Delta(w_i) = z_i$, $\Delta(z_i) = y_i$, $\Delta(y_i) = x_i$ and $\Delta(x_i) = 0$.

Here we need to know generators for $\mathbb{C}[R_1 \oplus mR_3]^{\mathrm{SL}_2(\mathbb{C})}$, the covariants of mR_3. The answer for $m = 2$, taken from von Gall [24], is given in Table 10.3.

F. von Gall [27] found generating covariants for $3R_3$. However by results of Schwarz [39, (1.22), (1.23)] (see also [47]) we may obtain all the generators of $\mathbb{C}[R_1 \oplus mR_3]^{\mathrm{SL}_2(\mathbb{C})}$ from the generators of $\mathbb{C}[R_1 \oplus 2R_3]^{\mathrm{SL}_2(\mathbb{C})}$ by the classical process of polarization. For a description of polarization see for example [35, Chapter 3, §2] or [47, p. 5]. Grace and Young [29, §257] also describe another procedure for finding generators for the covariants of $m\ R_3$.

It is straightforward to verify that polarization commutes with reduction modulo p. This implies that all the integral invariants of $\mathbb{F}_p[mV_4]^{C_p}$ are obtained from polarizing the 26 integral invariants in $\mathbb{F}_p[2V_4]^{C_p}$. In summary, if we let w_i, z_i, y_i, x_i denote a basis of the dual of the i^{th} copy of V_4 where $\Delta(w_i) = z_i$, $\Delta(z_i) = y_i$, $\Delta(y_i) = x_i$, $\Delta(x_i) = 0$ we have the following.

Theorem 10.7. *$\mathbb{F}_p[mV_4]^{C_p}$ is generated by*

- *$N^{C_p}(w_i)$ for $i = 1, \dots, m$;*
- *integral invariants arising from the polarizations of the 26 sources of the $\mathrm{SL}_2(\mathbb{C})$-invariants listed in Table 10.3.*
- *$\mathrm{Tr}(\prod_{i=1}^m y_i^{b_i} z_i^{c_i} w_i^{d_i})$ with $0 \le b_i \le 1$, $0 \le c_i \le p-1$ and $0 \le d_i \le p-1$.*

Table 3. Covariants of $R_3 \oplus R_3$

Covariant	Order	Bi-degree	LM	LM(Source)
f_1	3	$(1,0)$	a_0x^3	x_1
f_2	3	$(0,1)$	b_0x^3	x_2
$(f_1,f_2)^3$	0	$(1,1)$	a_3b_0	x_1w_2
H_{20}	2	$(2,0)$	$a_1^2x^2$	y_1^2
H_{11}	2	$(0,2)$	$a_2b_0x^2$	x_1z_2
H_{02}	2	$(1,1)$	$b_1^2x^2$	y_2^2
$U_{12} := (f_1,f_2)^1$	4	$(1,1)$	$a_1b_0x^4$	x_1y_2
$(f_1,H_{20})^1$	3	$(3,0)$	$a_1^3x^3$	y_1^3
$(f_2,H_{02})^1$	3	$(0,3)$	$b_1^3x^3$	y_2^3
$P := (f_2,H_{20})^2$	1	$(2,1)$	$a_2^2b_0x$	$y_1^2z_2$
$\pi := (f_1,H_{02})^2$	1	$(1,2)$	$a_2b_1^2x$	$x_1z_2^2$
$(f_1,H_{02})^1$	3	$(1,2)$	$a_1b_1^2x^3$	$x_1z_2y_2$
$(f_2,H_{20})^1$	3	$(2,1)$	$a_1a_2b_0x^3$	$y_1^2y_2$
$(H_{20},H_{20})^2$	0	$(4,0)$	$a_1^2a_2^2$	$z_1^2y_1^2$
$(H_{02},H_{02})^2$	0	$(0,4)$	$b_1^2b_2^2$	$z_2^2y_2^2$
$(H_{20},H_{02})^2$	0	$(2,2)$	$a_3^2b_0^2$	$x_1^2w_2^2$
$(H_{20},H_{11})^2$	0	$(3,1)$	$a_2^3b_0$	$y_1^3w_2$
$(H_{02},H_{11})^2$	0	$(1,3)$	$a_3b_1^3$	$x_1z_2^3$
$(f_1,P)^1$	2	$(3,1)$	$a_1a_2^2b_0x^2$	$y_1^2x_1w_2$
$(f_2,\pi)^1$	2	$(1,3)$	$a_3b_0b_1^2x^2$	$x_1z_2^2y_2$
$(H_{20},H_{02})^1$	2	$(2,2)$	$a_1a_2b_1^2x^2$	$y_1^2z_2y_2$
$(H_{20},P)^1$	1	$(4,1)$	$a_1a_2^3b_0x$	$y_1^4w_2$
$(H_{20},\pi)^1$	1	$(3,2)$	$a_1a_2^2b_1^2x$	$y_1^3z_2^2$
$(H_{02},P)^1$	1	$(2,3)$	$a_2^2b_1^3x$	$y_1^2z_2^2y_2$
$(H_{02},\pi)^1$	1	$(1,4)$	$a_3b_1^4x$	$x_1z_2^3y_2$
$(P,\pi)^1$	0	$(3,3)$	$a_2^2a_3b_0b_1^2$	$y_1^2x_1w_2z_2^2$

Remark 10.8. Shank [40, Theorem 3.2] showed that $\mathrm{LT}(\mathrm{Tr}(w_i^{p-1})) = z_i^{p-1}$. Thus we may use $\mathrm{Tr}(w_i^{p-1})$ in the role of f_{i1} when we apply Corollary 9.16 and hence we have $d_{i1} = p-1$ for all $i = 1,\dots,m$. This implies that we may restrict the values of the c_i to the range $0 \le c_i \le p-2$ in the third family of generators in the above theorem.

10.9. Other representations of C_p

There are a number of other $\mathrm{SL}_2(\mathbb{C})$-representations for which generators of the ring of covariants are known and thus for which we may compute the ring of invariants for the corresponding representation of C_p. Here we list some of these representations.

In 1869, Gordan [28] computed generators for the covariants of the quintic R_5 and the sextic R_6. Grace and Young [29, §116, §134] list these generators. In the 1880s F. von Gall gave generators for the covariants of the septic R_7 [26] and the octic R_8 [25]. Recently L. Bedratyuk computed generators for the covariants of the octic [11] and minimal generators for the covariants of the septic [10]. Thus we may list generators for the invariants of V_6, V_7, V_8 and V_9. Although Sylvester [45] published a putative list of generators for the covariants of the nonic R_9, a recent computation of the invariants of the nonic by A. Brouwer and M. Popoviciu [13] has shown Sylvester's table to be incorrect. The same two authors have also shown [14] that the ring of invariants of the decimic is generated by 106 invariants which they have constructed. Grace and Young [29, §138, §138A] give a method for obtaining generating covariants for $W \oplus R_1$ and $W \oplus R_2$ from the generating covariants of any representation W.

Acknowledgments. I thank R. J. Shank, Mike Roth and Gerry Schwarz for many helpful discussions. I also thank Megan Wehlau for a number of useful late night conversations which were the genesis of this work. This research is supported by grants from ARP and NSERC.

References

[1] Aitken, A. C.: The normal form of compound and induced matrices. Proc. London Math. Soc. **38**, 354–376 (1934) Zbl 0010.29102 MR 1576321

[2] Almkvist, G.: The number of nonfree components in the decomposition of symmetric powers in characteristic p. Pacific J. Math. 77 (1978), 293–301. Zbl 0417.20008 MR 0510925

[3] Almkvist, G.: Reciprocity theorems for representations in characteristic p. In: Séminaire d'Algèbre Paul Dubreil et Marie-Paule Malliavin, 32ème année (Paris, 1979), Lecture Notes in Math. 795, Springer, Berlin, 1–9 (1980) Zbl 0462.20010 MR 0582071

[4] Almkvist, G.: Invariants, mostly old. Pacific J. Math. **86**, 1–13 (1980) Zbl 0439.05005 MR 0586866

[5] Almkvist, G.: Representations of $\mathbb{Z}/p\mathbb{Z}$ in characteristic p and reciprocity theorems. J. Algebra **68**, 1–27 (1981) Zbl 0464.20008 MR 0604290

[6] Almkvist, G.: Some formulas in invariant theory. J. Algebra **77**, 338–359 (1982) Zbl 0492.20032 MR 0673120

[7] Almkvist, G.: Invariants of $\mathbb{Z}/p\mathbb{Z}$ in characteristic p. In: Invariant Theory (Montecatini, 1982), Lecture Notes in Math. 996, Springer, Berlin, 109–117 (1983) Zbl 0538.20003 MR 0718128

[8] Almkvist, G.: Representations of SL(2, $\mathbb{C}$) and unimodal polynomials. J. Algebra **108**, 283–309 (1987) Zbl 0624.20028 MR 0892905

[9] Almkvist, G., Fossum, R.: Decompositions of exterior and symmetric powers of indecomposable $\mathbb{Z}/p\mathbb{Z}$-modules in characteristic p. Lecture Notes in Math. 641, Springer, Berlin, 1–111 (1978) Zbl 0381.16015 MR 0499459

[10] Bedratyuk, L.: A complete minimal system of covariants for the binary form of degree 7. J. Symbolic Comput. **44**, 211–220 (2009) Zbl 1221.13006 MR 2479299

[11] Bedratyuk, L.: A complete system of covariants for the binary form of degree 8. Mat. Visn. Nauk. Tov. im. Shevchenka **5**, 11–22 (2008) (in Ukrainian)

[12] Benson, D. J.: Polynomial Invariants of Finite Groups. London Math. Soc. Lecture Note Ser. 190, Cambridge Univ. Press (1993) Zbl 0864.13001 MR 1249931

[13] Brouwer, A. E., Popoviciu, M.: The invariants of the binary nonic. J. Symbolic Comput. **45**, 709–720 (2010) Zbl 1189.13005 MR 2639312

[14] Brouwer, A. E., Popoviciu, M.: The invariants of the binary decimic. J. Symbolic Comput. **45**, 837–843 (2010) Zbl 1192.13005 MR 2657667

[15] Brualdi, R. A.: Combinatorial verification of the elementary divisors of tensor products. Linear Algebra Appl. **71**, 31–47 (1985) Zbl 0595.15023 MR 0813031

[16] Bryant, R. M., Kemper, G.: Global degree bounds and the transfer principle for invariants. J. Algebra **284**, 80–90 (2005) Zbl 1085.13001 MR 2115005

[17] Campbell, H. E. A., Fodden, B., Wehlau, D. L.: Invariants of the diagonal C_p-action on V_3. J. Algebra **303**, 501–513 (2006) Zbl 1115.13011 MR 2255119

[18] Campbell, H. E. A., Hughes, I. P.: Vector invariants of $U_2(\mathbb{F}_p)$: A proof of a conjecture of Richman. Adv. Math. **126**, 1–20 (1997) Zbl 0877.13004 MR 1440251

[19] Campbell, H. E. A., Shank, R. J., Wehlau, D. L.: Vector invariants for the two dimensional modular representation of a cyclic group of prime order. Adv. Math. **225**, 1069–1094 (2010) Zbl 1198.13009 MR 2671188

[20] Campbell, H. E. A., Wehlau, D. L.: Modular Invariant Theory. Encyclopaedia Math. 139, Springer (2011) Zbl 1216.14001 MR 2759466

[21] Cox, D., Little, J., O'Shea, D.: Ideals, Varieties, and Algorithms. Springer (1992) Zbl 0756.13017 MR 1189133

[22] Dickson, L. E. J.: On invariants and the theory of numbers. The Madison Colloquium (1913) Amer. Math. Soc., reprinted by Dover (1966) Zbl 0139.26603 MR 0201389

[23] Duncan, A., LeBlanc, M., Wehlau, D. L.: A SAGBI basis for $\mathbb{F}[V_2 \oplus V_2 \oplus V_3]^{C_p}$. Canad. Math. Bull. **52**, 72–83 (2009) Zbl 1181.13003 MR 2494313

[24] von Gall, F.: Die irreducibeln Syzyganten zweier simultanen cubischen Formen. Math. Ann. **31**, 424–440 (1888) JFM 20.0128.02

[25] von Gall, F.: Das vollständige Formensystem einer binären Form achter Ordnung. Math. Ann. **17**, 31–51 (1880) JFM 12.0093.02 MR 1510048

[26] von Gall, F.: Das vollständige Formensystem der binären Form 7^{ter} Ordnung. Math. Ann. **31**, 318–336 (1888) JFM 20.0128.01

[27] von Gall, F.: Das vollständige Formensystem dreier cubischen binären Formen. Math. Ann. **45**, 207–234 (1894) JFM 25.0186.02

[28] Gordan, P.: Beweis dass jede Covariante und Invariante einer binären Form eine ganze Function mit numerischen Coefficienten solcher Formen ist. J. Reine Angew. Math. **69**, 323–354 (1868)

[29] Grace, J. H., Young, A.: The Algebra of Invariants. Cambridge Univ. Press, Cambridge (1903) JFM 34.0114.01

[30] Hughes, I., Kemper, G.: Symmetric powers of modular representations, Hilbert series and degree bounds. Comm. Algebra **28**, 2059–2088 (2000) Zbl 0965.13004 MR 1747371

[31] Littlewood, D. E.: On induced and compound matrices. Proc. London Math. Soc. **40**, 370–381 (1936) Zbl 0013.04903 MR 1575831

[32] Marcus, M., Robinson, H.: Elementary divisors of tensor products. Comm. ACM **18**, 36–39 (1975) Zbl 0297.15025 MR 0364316

[33] Noether, E.: Der Endlichkeitssatz der invarianten endlicher Gruppen. Math. Ann. **77**, 89–92 (1915); reprinted in: Collected Papers, Springer, Berlin, 181–184 (1983) JFM 45.0198.01 MR 1511848

[34] Noether, E.: Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p. Nachr. Ges. Wiss. Göttingen **1926**, 28–35 JFM 52.0106.01

[35] Procesi, C.: Lie Groups. An Approach through Invariants and Representations. Universitext. Springer, New York (2007) Zbl 1154.22001

[36] Richman, D.: On vector invariants over finite fields. Adv. Math. **81**, 30–65 (1990) Zbl 0715.13002 MR 1051222

[37] Roberts, M.: On the covariants of a binary quantic of the nth degree. Quart. J. Pure Appl. Math. **4**, 168–178 (1861)

[38] Roth, W. E.: On direct product matrices. Bull. Amer. Math. Soc. **40**, 461–468 (1934) JFM 60.0056.01 MR 1562881

[39] Schwarz, G. W.: On classical invariant theory and binary cubics. Ann. Inst. Fourier (Grenoble) **37**, no. 3, 191–216 (1987) Zbl 0597.14011 MR 0916280

[40] Shank, R. J.: S.A.G.B.I. bases for rings of formal modular seminvariants. Comment. Math. Helv. **73**, 548–565 (1998) Zbl 0929.13001 MR 1639884

[41] Shank, R. J.: Classical covariants and modular invariants. In: H. E. A. Campbell and D. L. Wehlau (eds.), Invariant Theory in All Characteristics, CRM Proc. Lecture Notes 35, Amer. Math. Soc., 241–249 (2004) Zbl 1094.13008 MR 2066471

[42] Shank, R. J., Wehlau, D. L.: Noether numbers for subrepresentations of cyclic groups of prime order. Bull. London Math. Soc. **34**, 438–450 (2002) Zbl 1071.13001 MR 1897423

[43] Shank, R. J., Wehlau, D. L.: Computing modular invariants of p-groups. J. Symbolic Comput. **34**, 307–327 (2002) Zbl 1048.13002 MR 1937464

[44] Srinivasan, B.: The modular representation ring of a cyclic p-group. Proc. London Math. Soc. (3) **14**, 677–688 (1964) Zbl 0123.02801 MR 0168666

[45] Sylvester, J. J.: On the complete system of the "Grundformen" of the binary quantic of the ninth order. Amer. J. Math. **2**, 98–99 (1879) JFM 11.0081.03 MR 1505204

[46] Wehlau, D. L.: Weitzenböck derivations of nilpotency 3. Forum Math., DOI: 10.1515/forum-2011-0038 (2012)

[47] Weyl, H.: The Classical Groups, Their Invariants and Representations. Princeton Landmarks in Math., Princeton Univ. Press, Princeton, NJ (1997) Zbl 1024.20501 MR 1488158